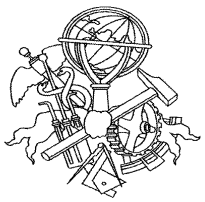
PROJECTO DE IMPLEMENTAÇÃO RFID NA EMPRESA ATEC

Manuel Fernando Gonçalves Teixeira



Mestrado em Engenharia Electrotécnica e de Computadores
Área de Especialização de Automação
Departamento de Engenharia Electrotécnica
Instituto Superior de Engenharia do Porto

2008

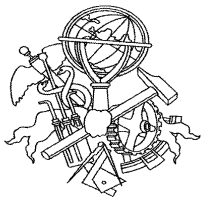
Este relatório refere-se à execução de uma Tese/Dissertação, do 2º ano, do Mestrado em Engenharia Electrotécnica e de Computadores

Candidato: Manuel Fernando Gonçalves Teixeira, Nº 1980337, 1980337@isep.ipp.pt

Orientação científica: Eng. Lino Manuel Baptista Figueiredo, lbf@isep.ipp.pt

Empresa: ATEC – Academia de Formação (Volkswagen / Bosch / Siemens / AHK)

Supervisão: Eng. Ricardo Gonçalves, ricardo.goncalves@atec.pt



Mestrado em Engenharia Electrotécnica e de Computadores

Área de Especialização de Automação

Departamento de Engenharia Electrotécnica

Instituto Superior de Engenharia do Porto

11 de Dezembro de 2008

Dedicado a ti.

Agradecimentos

Quero agradecer na parte da Orientação Cientifica ao Eng. Lino Figueiredo pelas palavras proferidas nos momentos certos para a execução da tese.

Deixo ainda uma palavra de gratidão ao Supervisor na Empresa, Eng. Ricardo Gonçalves, pela ajuda possível prestada no decurso.

Por último mas não menos importante à minha família, em especial à minha mulher pela paciência.

Resumo

A presente tese contém uma primeira parte que serve para contextualizar um pouco o projecto. Foi então feito o estudo do Estado da Arte do RFID (*Radio Frequency Identification*). Com isso pretende-se entrar em comparação de tecnologias existentes no mercado e tirar conclusões acerca da viabilidade de certas questões que devem ser levadas em conta. A segunda parte trata a implementação propriamente dita, na perspectiva da validação dos dados do controlo de acessos de activos da Academia de Formação ATEC. Através de equipamentos de leitura foi desenvolvido um software de reconhecimento, validação, tratamento e arquivo de dados para posterior consulta.

Palavras-Chave

RFID, Base de Dados.

Abstract

This Msc thesis has a first part to show some of the ways to the project. Therefore it has been made the study on the State of the Art in RFID (*Radio Frequency Identification*). Thus it is intended to compare different existent technologies, known at the market, and so to draw some conclusions about the viability on certain issues that must be taken into account. The second part deals with the implementation itself in order to validate data from the access control of ATEC Academy. Through reading equipment has been developed a software for recognition, validation, processing and archiving data for later reference.

Keywords

RFID, *Database*.

Résumé

Cette thèse contient une première partie qui sert à contextualiser un peu le projet. Donc ne l'étude de l'état de l'art dans la RFID (*Radio Frequency Identification*). Ainsi, il est destiné à comparer les technologies existantes sur le marché et d'en tirer des conclusions quant à la viabilité de certaines des questions qui doivent être prises en compte. La deuxième partie traite de la mise en œuvre elle-même, en vue de la validation des données du contrôle de l'accès aux éléments d'actif de l'Académie de Formation ATEC. Grâce à des appareils de lecture a été mis au point un logiciel de reconnaissance, de validation, de traitement et d'archivage de données pour référence ultérieure.

Mots-clés

RFID, *Base de Données*.

Índice

Índice de Figuras

Índice de Tabelas

Acrónimos

RFID	*Radio Frequency Identification*
EPC	*Electronic Product Code*
IFF	*Identify Friend or Foe*
EAS	*Electronic Article Surveillance*
EAN	*European Article Number*
ISO	*International Normas Organization*
RF	*Radio Frequency*
CMOS	*Complementary Metal Oxyde Semiconductor*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*
UHF	*Ultra High Frequency*
RO	*Read Only*
WORM	*Write Once Read Many*
RW	*Read-Write*
EPC	*Electronic Product Code*
FRAM	*Ferroelectric Random Access Memory*
EBE	*Enterprise Back-End*
ERP	*Enterprise Resource Planning*
WMS	*Web Map Service*

.NET	*Microsoft's web services architecture*
API	*Application Programming Interface*
ALE	*Application Layer Event*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
SMTP	*Simple Mail Transfer Protocol*
MSMQ	*Microsoft Message Queue*
BM	*Business Modules*
SQL	*Structured Query Language*
LDAP	*Lightweight Directory Access Protocol*
DPP	*Distributed Parallel Processing*
MP	*Multiprotocol*
FDX	*Full Duplex*
HDX	*Half Duplex*
SEQ	Sequencial
RSA	*Resource Source Authentication*
EMEA	Europa Médio Oriente e África
RTLS	*Real Time Location Systems*
HF	*High Frequency*
LF	*Low Frequency*
VHF	*Very High Frequency*

VLF	*Very Low Frequency*
SDK	*Standard Development Kit* – Biblioteca de Desenvolvimento
Firmware	*Software* entre o *hardware* e o utilizador, mais ligado a *hardware*

1. INTRODUÇÃO

O elevado desenvolvimento tecnológico dos últimos anos trouxe à luz do dia cada vez maiores e mais complexos desafios. O mundo das telecomunicações necessita constantemente de novas técnicas e tecnologias, tal a ânsia das pessoas em obter os melhores meios de comunicação, mais modernos e com maiores capacidades. Qualquer pessoa usa, sem se aperceber, instrumentos de comunicação, desde o mais simples e vulgar telefone ao mais complexo e sofisticado telemóvel de tamanho consideravelmente reduzido. Nas grandes empresas e em instituições governamentais, essa ânsia por mais e melhores meios de comunicação leva ao ainda mais exigente patamar da RFID (*Radio Frequency Identification)*, pois a posição de cada membro de uma equipa ou a localização de um bem essencial pode ser fulcral para reduzir drasticamente o tempo de uma acção. Esta imposição de rapidez de actos que leva a uma necessidade absoluta de conhecer todos os meios necessários a uma determinada tarefa ou trabalho, faz com que as grandes empresas de todo o mundo apostem e direccionem os seus recursos, cada vez mais para esta área. O RFID pode ser caracterizado como uma tecnologia evolucionária, isto porque o seu grande objectivo deverá ser o de, parcialmente substituir o código de barras (o concorrente comparativo mais directo), tornando assim possível alcançar uma maior produtividade, fruto da automatização de inúmeros processos. O seu leque de aplicações é tão abrangente que existem debates importantes sobre os efeitos e impactos sociais que a

forte implementação da RFID poderá criar na sociedade actual [1]. Contudo, uma perda significativa de privacidade individual poderá não ser bem encarada por alguns. Existindo um equilíbrio, a utilidade é inquestionável, o crescimento inevitável e a aposta no desenvolvimento de novos, mais pequenos e mais abrangentes dispositivos também. Ao nível dos custos associados à implementação da tecnologia, estes têm reduzido de forma acentuada, fruto da grande quantidade de encomendas que têm sucedido no mercado. A tecnologia encontra-se em fase de amadurecimento e, como tal, a procura irá suplantar em muito as actuais necessidades. Convém igualmente referir algumas das questões essenciais para que o RFID evolua para a fase seguinte. Em primeiro lugar será necessário estabilizar e uniformizar normas. Existem actualmente vários grupos de discussão, constituídos por empresas de renome do sector, que se encontram a definir arquitecturas, protocolos, frequências de operação, etc. Finalmente, do ponto de vista dos modelos de negócio, estes deverão ser estudados e desenvolvidos para que toda esta lógica de processamento possa depois ser aplicada à informação recolhida pelo RFID.

1.1 CONTEXTUALIZAÇÃO

Este projecto surgiu da necessidade da Academia de Formação ATEC em implementar um sistema que pudesse controlar as horas de entrada e saída de todos os seus activos. Assente numa base de formação em sala, tornou-se inquestionável a ideia de se saber em tempo real, ou em arquivo (dependendo do momento), quais os comportamentos em termos de assiduidade e pontualidade dos seus activos internos (funcionários) bem como dos seus externos (formandos e formadores/prestadores de serviços). Alem do projecto foi feito um estudo completo da tecnologia no seu Estado de Arte actual.

1.2 OBJECTIVOS

Um dos objectivos deste projecto é a aquisição futura do equipamento necessário à execução, referida na contextualização. O controlo de assiduidade e pontualidade é premente nas instalações da empresa ATEC, e por isso para além da análise do estado da arte da tecnologia (parte inicial da tese), foram procurados no mercado os equipamentos de escolha prioritária com consequente estudo de custos/opções tecnológicas, de forma a compatibilizar *software* já desenvolvido. Dada a complexidade foi feita uma subdivisão das tarefas, tais como:

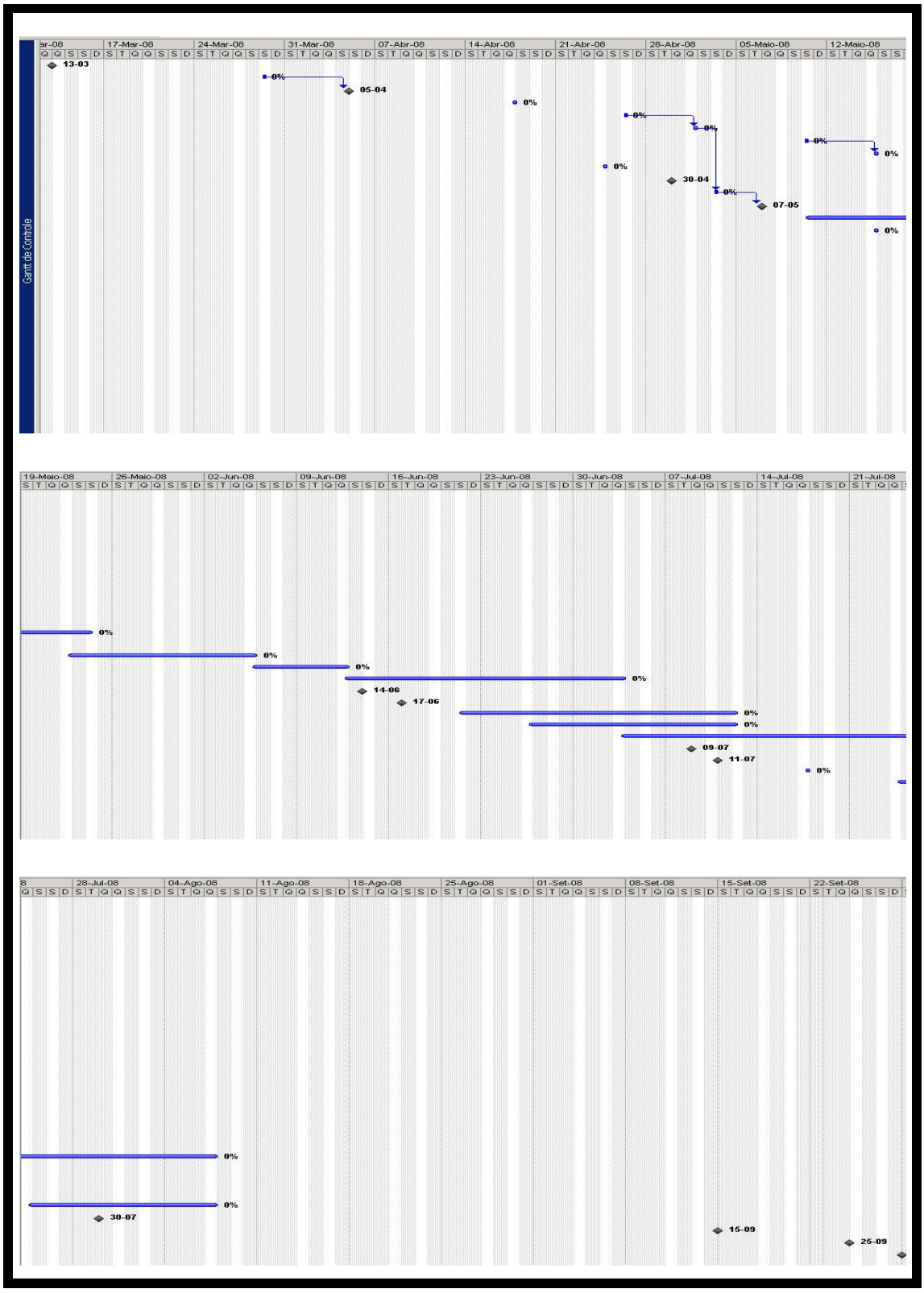
- O estudo do Estado da Arte relativo a RFID;
- Prós e Contras da sua Utilização;
- Aplicações (Comparação);
- Estudo de Mercado (Equipamentos)
- Projecto estrutural de Implementação
- Desenvolvimento *Software*

1.3 CALENDARIZAÇÃO

Sendo este trabalho realizado numa conjuntura teórico-prática procedeu-se ao estudo do Estado da Arte numa primeira fase e ao projecto posteriormente, sendo assim a sua prossecução conduziu à calendarização apresentada na Tabela 1. As tarefas estão precisamente divididas segundo a lógica acima explicada. As datas poderão ser afectadas em relação à previsão por indisponibilidade de pessoas e/ou informação.

Tabela 1 Calendarização do Projecto

	Nome da Tarefa	Duração	Início	Término
1	Apresentação 1a Etapa Tese (Estado Arte) / Reunião ATEC de definição conteúdos	0 dias	Qui 13-03-08	Qui 13-03-08
2	Pesquisa possibilidades de concretização e integração	1 dia	Sáb 29-03-08	Sáb 29-03-08
3	Reunião ISEP com coordenador cientifico: Engenheiro Lino Figueiredo	0 dias	Sáb 05-04-08	Sáb 05-04-08
4	Definição parâmetros concretos e possibilidades de execução	1 dia	Qui 17-04-08	Qui 17-04-08
5	Análise de mercado de empresas hardware	1 dia	Sáb 26-04-08	Sáb 26-04-08
6	Marcação reuniões com empresas contactadas	1 dia	Qui 01-05-08	Qui 01-05-08
7	Reunião com Telemax	1 dia	Sáb 10-05-08	Sáb 10-05-08
8	Reunião com Netponto	1 dia	Qui 15-05-08	Qui 15-05-08
9	Reunião com Bioglobal	1 dia	Qui 24-04-08	Qui 24-04-08
10	Reunião ATEC apresentação de dados	0 dias	Qua 30-04-08	Qua 30-04-08
11	Decisão adopção equipamento IDTECK - Telemax	1 dia	Sáb 03-05-08	Sáb 03-05-08
12	Reunião ISEP Coordenador Cientifico apresentação de dados	0 dias	Qua 07-05-08	Qua 07-05-08
13	Análise completa de caracteristicas de equipamento IDTECK	5 dias	Sáb 10-05-08	Sáb 24-05-08
14	Aperfeiçoamento Primeira Etapa Tese	1 dia	Qui 15-05-08	Qui 15-05-08
15	Recepção de software gestão de assiduidades actualizado IDTECK	5 dias	Qui 22-05-08	Qui 05-06-08
16	Reunião Engenheiro Lino para direccionamento Tese	3 dias	Qui 05-06-08	Qui 12-06-08
17	Desenvolvimento software Gestão de Assiduidades	7 dias	Qui 12-06-08	Qui 03-07-08
18	Reunião ATEC apresentação desenvolvimento software	0 dias	Sáb 14-06-08	Sáb 14-06-08
19	Reunião ISEP apresentação desenvolvimento software	0 dias	Ter 17-06-08	Ter 17-06-08
20	Conexão base de dados à plataforma de software anteriormente desenvolvida	7 dias	Sáb 21-06-08	Sáb 12-07-08
21	Redefinições Conteúdos Tese	6 dias	Qui 26-06-08	Sáb 12-07-08
22	Desenvolvimento Sofware	11 dias	Qui 03-07-08	Qui 07-08-08
23	Reunião ATEC apresentação conteúdos Tese	0 dias	Qua 09-07-08	Qua 09-07-08
24	Reunião ISEP apresentação conteúdos Tese	0 dias	Sex 11-07-08	Sex 11-07-08
25	Recolha Documentação Cientifica	1 dia	Qui 17-07-08	Qui 17-07-08
26	Tratamento Documentação Cientifica	5 dias	Qui 24-07-08	Qui 07-08-08
27	Reunião ATEC apresentação fase Documentação	0 dias	Qua 30-07-08	Qua 30-07-08
28	Reunião ISEP pré-apresentação final	0 dias	Seg 15-09-08	Seg 15-09-08
29	Apresentação Relatório Tese	0 dias	Qui 25-09-08	Qui 25-09-08
30	Apresentação Equipa Avaliativa Júris ISEP	0 dias	Seg 29-09-08	Seg 29-09-08


Gantt de Controle
17-Mar-08
24-Mar-08
31-Mar-08
07-Abr-08
14-Abr-08
21-Abr-08
28-Abr-08
05-Maio-08
12-Maio-08
13-03
05-04
30-04
07-05
19-Maio-08
26-Maio-08
02-Jun-08
09-Jun-08
16-Jun-08
23-Jun-08
30-Jun-08
07-Jul-08
14-Jul-08
21-Jul-08
14-06
17-06
09-07
11-07
28-Jul-08
04-Ago-08
11-Ago-08
18-Ago-08
25-Ago-08
01-Set-08
08-Set-08
15-Set-08
22-Set-08
30-07
15-09
25-09

1.4 ORGANIZAÇÃO DO RELATÓRIO

O desenvolvimento do sistema RFID proposto na corrente tese implica um profundo e esquematizado estudo das tecnologias, princípios de funcionamento e principais características dos seus elementos constituintes, bem como dos seus comportamentos para as situações ponderadas. É fundamental começar por um estudo cuidado do universo da tecnologia em análise, sendo assim apresentado um Estado da Arte RFID actual, desde a sua história, constituição dos sistemas, modos de funcionamento entre outros, de forma a melhor inserir e enquadrar o sistema proposto no meio tecnológico a que se destina.

O primeiro capítulo introduz a tecnologia.

O segundo capítulo dá a conhecer o Estado da Arte.

O terceiro capítulo é dedicado à segurança e futuro desta.

O quarto capítulo apresenta as aplicações mais comuns.

O quinto capítulo expõe a implementação na empresa.

O sexto capítulo caracteriza as conclusões e as perspectivas de desenvolvimento futuro.

2. ESTADO DA ARTE RFID

Uma onda rádio é uma onda electromagnética e é criada por electrões em movimento que consistem na oscilação de campos eléctricos e magnéticos, permitindo transportar energia de um ponto para o outro, propagando-se através de vários tipos de materiais. Em física, comprimento de onda é a distância entre valores repetidos num padrão de onda sinusoidal. Chama-se a uma oscilação completa da onda, um ciclo de onda. O tempo que uma onda demora a fazer este ciclo é chamado o período de oscilação, e o número de ciclos num segundo chama-se **frequência**. A frequência de uma onda é medida em hertz (abreviado [**Hz**]=ciclos/segundo). Nome dado em honra ao físico Alemão Henrich Rudolg Hertz. A amplitude é a altura do pico da onda [39].

Informação adicional:

1 Kilo Hertz [k**Hz**] = 1 000 Hertz

1 Mega Hertz [M**Hz**] = 1 000 000 Hertz

1 Giga Hertz [G**Hz**] = 1 000 000 000 Hertz

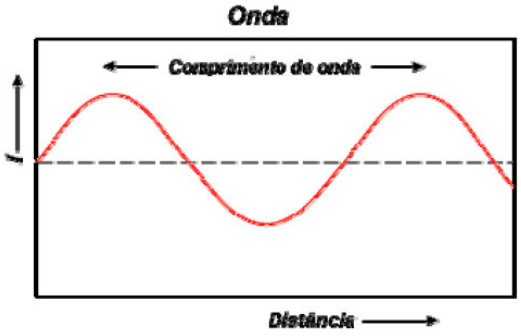


Figura 1 Onda Sinusoidal [39]

A tabela 2 refere-se às propriedades de alguns materiais que trabalham precisamente com as ondas explicitadas e às frequências, que neste caso, são as mais utilizadas pelo RFID, situando-se entre 30 kHz e os 5,8 GHz.

Material	LF	HF	UHF	Microondas
Roupa				
Madeira seca				
Grafite				
Líquidos				
Metais				
Óleo de motor				
Produtos de papel				
Plástico				
Água				
Madeira húmida				

Absorve RF
Opaco à RF
Condutor de RF

Tabela 2 Propriedades de materiais em relação aos espectros [39]

Os materiais denominados por condutores são os que permitem que a onda os atravesse sem causar uma perda significativa de energia. Os materiais absorventes são os que permitem a propagação da onda, contudo causam grandes perdas de energia da onda, por último os materiais opacos são os que reflectem e bloqueiam por completo a propagação da onda [39]. Qualquer destes materiais pode estar num dispositivo RFID.

RFID é um acrónimo do nome ***R**adio-**F**requency **ID**entification* em inglês que, em português, significa **Identificação por Rádio Frequência**. Trata-se de um método de identificação automática através de sinais de rádio, recuperando e armazenando dados remotamente através de dispositivos chamados de *tags* RFID [1]. Uma *tag* RFID é um pequeno objecto, que pode ser colocado numa pessoa, animal ou produto. Contém chips de silício e antenas, exemplo na figura 2, que lhe permite responder aos sinais de rádio enviados por uma base transmissora [9].

Figura 2 Etiquetas RFID

Associadas muitas vezes, à gestão do inventário e de abastecimento, as aplicações de Identificação por Rádio Frequência (RFID) estão a crescer de forma rápida. Desde as instalações fabris aos veículos, passando pelos aeroportos militares até às estantes das lojas e cabinas de portagem, o RFID está firmemente a transformar a maneira como o mundo actual funciona [6].

Os sistemas RFID podem funcionar sem intervenção humana fornecendo informação precisa, objectiva, fiável e totalmente auditável. Os dados podem facilitar melhorias nos processos, nomeadamente a realização de prognósticos [8]. No meio logístico, a tecnologia é usada para controlar a entrada e saída de mercadorias e para gerir o espaço de armazém. No meio dos transportes, usa-se para identificar veículos, como por exemplo nos transportes ferroviários, para controlo do funcionamento dos sinais, das cancelas nas passagens de nível e registar a entrada e saída dos comboios nas estações.

Só faz sentido usar RFID, se os utilizadores confiarem na tecnologia. A confiança é conseguida quando o utilizador verifica as vantagens que a tecnologia trouxe ao seu negócio. As soluções aplicacionais (*hardware* e *software*) têm o objectivo de oferecer serviços e ferramentas que permitam gerir a arquitectura implementada. Têm ainda a capacidade para baixar custos e subir a eficácia com maior atenção dada ao cliente, conseguindo-se retornos mais satisfatórios com recursos que dirigem operações [1].

Existem no entanto algumas questões que devem ser levadas em linha de conta para a execução de projectos deste género como se apresenta na tabela 3, devidamente categorizadas por classificação.

Normas	Custos	Tecnologia	Oferta	Processos	Cooperação	Consumidores
Harmonização	Etiquetas	Capacidade de Processamento	Chips	Revisão de Processos	Fornecedores	Privacidade
Global	Leitores	Absorção por líquidos	Leitores	Custos Totais	Distribuidores	Saúde
Interoperabilidade						
Entre sistemas	Sistemas de Informação	Reflexão por metal	Software	Interligação com Actividades e Sistemas	Vendas e Clientes	Ambiente

Tabela 3 Questões colocadas por um sistema RFID

Actualmente as *tags* EPC (*Electronic Product Code*), adiante explicitadas, de 96 bits permitem gerar cerca de 80 000 x 10^{36} números de identificação. Portanto um número

pequeno de bits pode virtualmente identificar todos os tipos de objectos no mundo. Contudo o que torna esta tecnologia bastante apelativa é o facto de esta informação estar disponibilizada à distância e em dimensões bastante reduzidas [39].

Antes de se começar a planear a implementação de um sistema como este, devem-se ter em conta os custos, nomeadamente e numa primeira fase os de *Hardware* (Etiquetas, Leitores, Antenas, PC's, etc). Existirão ainda problemáticas económicas relacionadas com *software*, adaptação das pessoas ao respectivo sistema e ainda de normalização. Alem disso há que lançar questões que se prendem com Privacidade, Saúde e Ambiente.

2.1 RFID NOS TEMPOS

Em 1906, Ernst F.W. Alexanderson, demonstrou a primeira onda contínua através da criação e transmissão de sinais de rádio. Marcou o começo da comunicação de rádio moderna, onde todos os aspectos das ondas de rádio são controlados. Ainda no início do mesmo século, tivemos a descoberta do radar. Durante a Segunda Guerra Mundial, através de um projecto denominado "Projecto Manhattan", que o aperfeiçoou, foi possível intensificar o avanço da tecnologia de RFID, que através do envio de ondas de rádio, podia descobrir e localizar um objecto através da reflexão, determinando a sua posição e a velocidade. Considerando que uma forma de RFID, é a combinação da tecnologia de radiodifusão e do radar, é certo que as convergências destes dois, contribuíram para o aprimoramento [37]. Os alemães, japoneses, americanos e ingleses utilizavam radares – que foram descobertos em 1937 por Sir Robert Alexander Watson-Watt, um físico escocês – para avisá-los com antecedência de aviões enquanto eles ainda estavam distantes. O problema era identificar quais desses aviões eram inimigos e quais eram aliados. Os alemães então descobriram que se os seus pilotos virassem os aviões quando estavam a regressar à base iriam modificar o sinal de rádio que seria reflectido para o radar. Este método simples alertava os técnicos responsáveis que se tratavam de aviões alemães (e este foi, essencialmente, considerado o primeiro sistema passivo de RFID) [9].

Em 1948, foi publicado o primeiro trabalho que explorava o RFID através de Harry Stockman, sob o título de *Communication by Means of Reflected Power*. Evidentemente outras pesquisas, deveriam ainda contribuir muito para eliminar os problemas existentes na época, antes de explorar a tecnologia num vasto campo de aplicações úteis [37]. Sob o comando de Watson-Watt, os ingleses desenvolveram o primeiro identificador activo de

amigo ou inimigo (**IFF** – ***I****dentify* ***F****riend or* ***F****oe*). Foi colocado um transmissor em cada avião britânico e quando esses transmissores recebiam sinais das estações de radar no solo, começavam a transmitir um sinal de resposta, que identificava o objecto como *Friendly* (amigo). Os RFID funcionam no mesmo princípio básico. Um sinal é enviado a um *transponder*, o qual é activado e reflecte de volta o sinal (sistemas passivos) ou transmite o seu próprio sinal (sistemas activos) [8].

Avanços na área de radares e de comunicação RF (*Radio Frequency*) continuaram através das décadas de 50 e 60.

Os anos 60 foram o prelúdio da explosão do RFID dos anos 70.

R.F. Harrington estudou a teoria electromagnética relacionada com o RFID, e editou em 1964 um documento denominado: *Theory of Loaded Scatterers*. Outros grandes avanços na época foram as descobertas publicadas por Robert Richardson's, sobre activação remota de dispositivos, e o aprofundamento das técnicas de transmissão de dados passivas publicadas por J.H. Vogelman's. No início dos anos 70, fomentadores, inventores, companhias académicas e laboratórios do governo, estavam a trabalhar activamente na tecnologia. Em 1975, foi apresentado para a comunidade por Alfred Koelle, Steven Depp e Robert Freyman, um importante estudo sobre RFID, originalmente com o título: *Short-Range Radio-Telemetry for Electronic Identification Using Modulated Backscatter*. Este desenvolvimento sinalizou o começo práctico do uso das etiquetas, completamente passivas e com amplitude operacional até dez metros. No mesmo ano, as autoridades dos portos de Nova Iorque e de Nova Jersey, testaram sistemas construídos pela General Electric, Westinghouse, Philips e Glenayre. Os resultados foram favoráveis, mas a sua primeira aplicação com sucesso para utilização no transporte comercial foi numa estação de autocarros, com restrições de uso nos horários de grandes movimentos [37].

A década de 80, foi marcada por várias implementações utilizando a tecnologia RFID. Ainda sem a definição dos padrões, é marcada por diferentes interesses em várias partes do mundo. O *Massachusetts Institute of Technology* (MIT), juntamente com outros centros de pesquisa, iniciou o estudo de uma arquitectura que utilizasse os recursos das tecnologias baseadas em radiofrequência para servir como modelo de referência ao desenvolvimento de novas aplicações de perseguição e localização de produtos. Desse estudo, nasceu o Código Electrónico de Produtos - EPC (*Electronic Product Code*). O EPC definiu uma

arquitectura de identificação de produtos que utilizava os recursos proporcionados pelos sinais de radiofrequência, chamada posteriormente de RFID [37].

Nos Estados Unidos, os maiores interessados nesta tecnologia, desenvolveram aplicações para transportes, controlos de acesso de pessoal, e com menos ênfase as aplicações para o controlo de animais. Na Europa os maiores interessados, trabalhavam em sistemas utilizando-os em controlo de animais (com alcance limitado), e diversas outras aplicações industriais e empresariais. Entretanto teve destaque a aplicação da tecnologia de RFID no controlo de passagem nas praças e estradas em Itália, França, Espanha, Portugal e Noruega. Ainda na década de 80, o que determinou a expansão rápida das aplicações, foi o desenvolvimento do computador pessoal, que acelerou de maneira rápida e económica, a colecção conveniente dos dados [37].

Os anos 90 foram marcados pela multiplicação das aplicações comerciais utilizando RFID nas paragens de transportes nos Estados Unidos, e em sistemas com etiquetas inteligentes instaladas em postos de gasolina em Kansas e Oklahoma. Ainda na década de 90, com a expansão comercial, teve início o uso das etiquetas multi-protocolo, bem como o uso de uma única etiqueta por veiculo, identificando um bilhete único em várias localizações de transportes de diferentes estradas, pontes, túneis, sob juridição de diversas autoridades regionais. Ainda na Europa, a tecnologia evoluiu nos anos 90, tal qual o crescimento alcançado na América do Norte, em aplicações comerciais, com esforço de desenvolvimento das grandes empresas como: Texas Instruments, Microdesign, Alcatel, Bosch e subsidiárias da Philips. Em muitos outros países do mundo, estavam a aparecer aplicações que utilizavam a tecnologia de RFID. Dos países que iniciaram o uso pode-se citar: Austrália, China, Hong Kong, Filipinas, Argentina, México, Brasil, Canadá, Japão e Singapura.

Outros estudos levam ao surgimento no mercado dos primeiros EAS (*Electronic Article Surveillance*) que têm como objectivo impedir o furto em superfícies comerciais. Companhias começam a comercializar sistemas anti-roubo que utilizam ondas de rádio para determinar se um item havia sido roubado ou pago normalmente. Era o advento das *tags* (etiquetas) denominadas de "etiquetas de vigilância electrónica" as quais ainda são utilizadas até hoje. Cada etiqueta utiliza um bit. Se a pessoa paga pela mercadoria, o bit é posto em *off* ou 0, e os sensores não dispararão o alarme. Caso contrário, o bit continua em *on* ou 1, e caso a mercadoria saia através dos sensores, um alarme será disparado [9]. Os

avanços tecnológicos permitiram a construção de novos circuitos integrados, que asseguraram a utilização das etiquetas inteligentes em maior escala, nos segmentos comerciais. O século 21 iniciou com o uso crescente das etiquetas inteligentes, em virtude da redução dos custos, da ampliação das funcionalidades e o aumento da confiança. As contribuições para a padronização desta tecnologia, estão em andamento e são conduzidas pelos centros de pesquisas e divulgações como o *Massachusetts Institute Technology*, pelos fabricantes de equipamentos para RFID, por pesquisadores e utilizadores interessados na padronização. Repare-se que esta é uma tecnologia que atravessa sistemas, ampliando o desenvolvimento de software, teoria de circuito, teoria de antena, propagação de rádio, técnica de microondas, modelo de receptor, modelo de circuito integrado, criptografia, tecnologia de materiais, modelo mecânico, e engenharia de rede. Números crescentes de engenheiros são envolvidos no desenvolvimento de aplicações de RFID, e esta tendência provavelmente continuará [37].

- Patentes RFID

No que diz respeito a patentes Mario W. Cardullo requereu a primeira patente para uma etiqueta activa de RFID com uma memória regravável em 23 de Janeiro de 1973. Nesse mesmo ano, Charles Walton, um empreendedor da Califórnia, recebeu a patente por um *transponder* passivo usado para destrancar uma porta sem a utilização de uma chave. Um cartão com um *transponder* embutido comunicava com um leitor/receptor localizado perto da porta. Quando o receptor detectava um número de identificação válido armazenado na etiqueta RFID, a porta era destrancada através de um mecanismo.

No começo da década de 90, engenheiros da IBM desenvolveram e patentearam um sistema de RFID baseado na tecnologia UHF (*Ultra High Frequency*). O UHF oferece um alcance de leitura bastante maior (aproximadamente 6 m sob condições boas) e transferências de dados mais velozes. Apesar de realizar testes com a rede de supermercados Wal-Mart, não chegou a comercializar essa tecnologia. Em meados de 1990, a IBM vendeu a patente para a Intermec, um provedor de sistemas de código de barras. Após isso, o sistema de RFID da Intermec tem sido instalado em inúmeras aplicações diferentes, desde armazéns até à agricultura. Mas a tecnologia era muito cara comparada com o pequeno volume de vendas, e a falta de interesse internacional. O RFID a utilizar UHF tem uma melhoria na sua visibilidade em 1999, quando o *Uniform Code Council*, o EAN internacional, a Procter & Gamble e a Gillette se uniram e estabeleceram

o Auto-ID Center, no Instituto de Tecnologia de Massachusetts. Dois professores, David Brock e Sanjay Sarma, têm realizado pesquisas para viabilizar a utilização de etiquetas de RFID de baixo custo em todos os produtos feitos e ter controlo sobre estes. A ideia consiste em colocar apenas um número de série em cada etiqueta para manter o preço baixo (utilizando apenas um *microchip* simples que armazenaria pouca informação). A informação associada ao número de série de cada etiqueta pode ser armazenada em qualquer banco de dados externo, acessível inclusive pela Internet [9]. Na tabela 4 pode ser vista uma representação temporal da tecnologia. Assim se passou até hoje.

2.1.1 Cronologia

Década	Eventos
1940-1950	Invenção e rápido desenvolvimento do radar durante a 2ª Guerra Mundial Início de funcionamento do RFID em 1948
1950-1960	Primeiras explorações da RFID e experiências laboratoriais
1960-1970	Desenvolvimento da teoria da RFID Primeiras aplicações experimentais no terreno
1970-1980	Explosão no desenvolvimento da RFID; Aceleração dos testes Implementações embrionárias de RFID
1980-1990	Aplicações comerciais de RFID entram no mercado
1990-2000	Surgimento de normas RFID é largamente utilizado começando a fazer parte da vida de cada um
2000-2008	Vulgarização do uso do RFID Inicio abrupto do fabrico da tecnologia a tamanhos reduzidos para integração em aplicações das mais diversas possível

Tabela 4 Quadro-resumo (por décadas) da história do RFID.

Cronologicamente pode-se verificar que ao longo dos tempos o RFID teve uma escalada de utilização. Não se trata de uma tecnologia propriamente histórica pois ainda não conta com séculos de experiência, mas mesmo assim já se encontra bastante desenvolvida. A partir da Segunda Grande Guerra dá-se a escalada tecnológica, devido à utilização das emissões *on-the-air* e o que se segue são experiências, testes e tentativas de uniformização (normas para controlo dos parâmetros envolventes) até à sua vulgarização com tamanhos a nível micro tecnológico. Como se pode ver a tecnologia foi-se propagando e divulgando até chegarmos ao patamar de diversidade de aplicações de que dispomos hoje. Algumas delas foram inclusive o trampolim para que o RFID começasse a ser aceite e usado em grande escala. A figura 3 é isso que documenta, juntamente com as maiores tendências de aplicação em 2008.

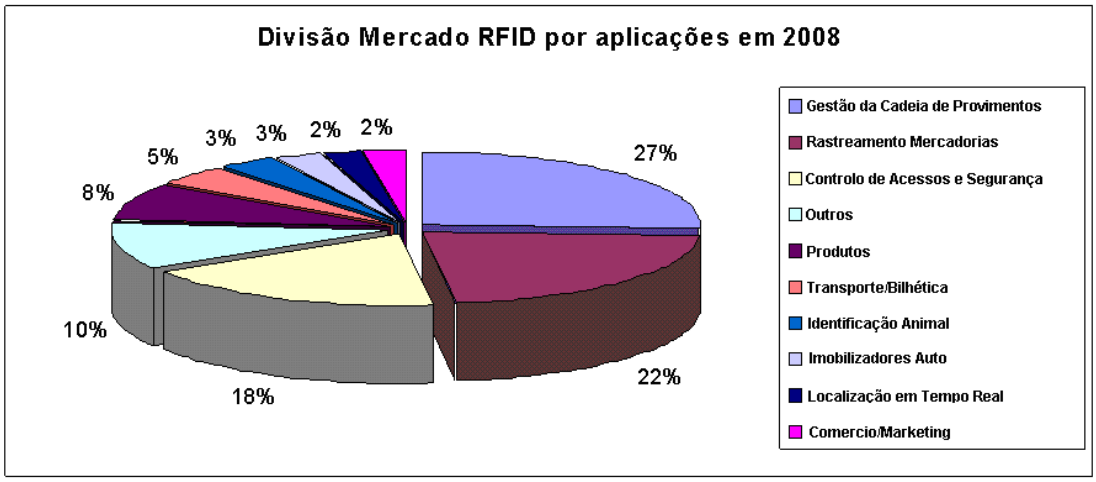


Figura 3 Mercado RFID por aplicação [33]

2.2 EQUIPAMENTO

Toda a infra-estrutura RFID é composta por diversos componentes, os quais são aqui brevemente apresentados. Os sistemas de RFID que se encontram actualmente no mercado têm uma arquitectura bastante simples, e que se baseia em quatro componentes básicos – O *Tag*, a *Antena*, o Leitor (*Reader*) e um módulo de *middleware* (típico para controlo das variáveis) [2]. No entanto os dois principais blocos do sistema são: o *Tag* e o *Reader*

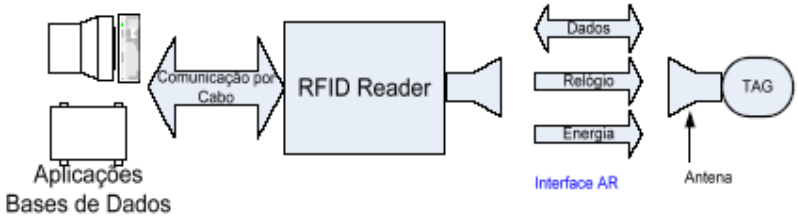


Figura 4 Esquema dos dois blocos e interligações típicas [2]

O *tag* (ou *transponder*) é um pequeno dispositivo que serve de identificador do objecto no qual foi implementado. Quando solicitado pelo *reader*, devolve a informação contida dentro do seu pequeno *microchip*, quer esta seja apenas um simples bit ou uma pequena base de dados identificativos do histórico do produto. Note-se, contudo, que apesar deste ser o método mais comum, existem *tags* activos que transmitem informação sem a presença do *reader*. O *reader* pode ser considerado o "cérebro" de um sistema RFID [2]. Isto porque, sendo o responsável pela ligação entre sistemas externos de processamento de dados (computadores com base de dados) e os *tags*, é também da sua responsabilidade a

gestão do sistema. Essa gestão pode passar por controlo de acesso múltiplo (de vários *tags*), rejeição de repetições de dados, correcção de erros, entre outros. A razão da grande maioria destes processamentos serem colocados no *reader,* advém do facto de o *tag* ser um dispositivo de tamanho reduzido e baixa complexidade (baixo custo), pelo que todos os mecanismos de segurança, gestão e controlo do sistema deverão ser colocados no *reader.* Por isso, o *reader* é naturalmente de maior dimensão, de maior complexidade e de maior custo, pelo que num sistema básico de RFID pode existir apenas um *reader* para dezenas ou centenas de *tags* [2].

2.2.1 Tags

Estes elementos em diversidade representam já um universo superior a 500 sub-categorias diferentes [29]. São pequenos cartões ou peças de plástico, também conhecidos por de proximidade, que podem ser encontrados sob diferentes formatos: passivos, semi-passivos ou activos. As suas dimensões e aplicações variam consoante o formato, pelo que é descrito, de forma breve, cada um deles. No entanto, cada um destes formatos não deve ser visto como alternativa aos outros, mas antes como tecnologias complementares.

2.2.1.1 Tags Passivas

As *tags* passivas não necessitam de qualquer tipo de alimentação, pelo que passam a maior parte do tempo "adormecidas". Apenas quando se encontram numa zona de leitura (*Read Zone*), constituída por uma antena ligada a um *reader*, são activadas por via da potência emitida pela antena [4]. É através desta potência RF emitida que a *tag* "acorda" e, reaproveitando essa mesma energia para o circuito integrado CMOS, retransmite informação [2]. O *microchip* de um *tag* passivo tem que possuir obrigatoriamente um controlador/rectificador de potência de forma a converter a potência AC do sinal RF em potência DC. Possui também um extractor de relógio e um modulador que modula a onda recebida do *reader*. O *microchip* possui ainda uma unidade lógica que é responsável pela implementação do protocolo de comunicação entre o *tag* e o *reader*, e uma memória interna para armazenamento de dados [2] (figura 5).

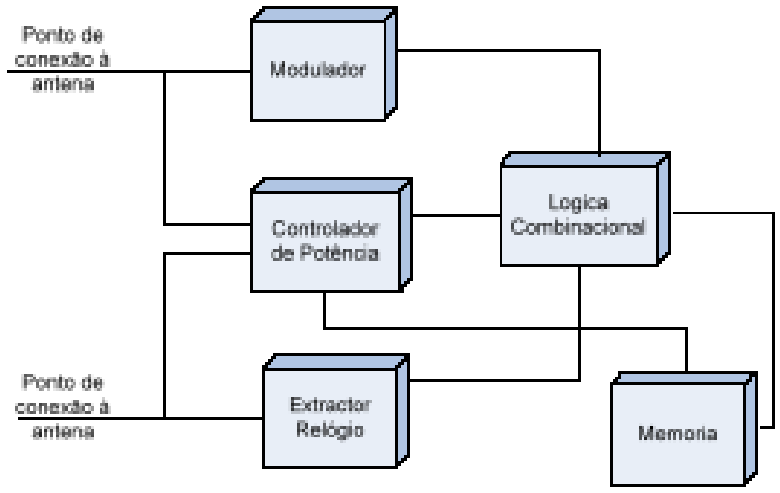


Figura 5 Componentes básicos do microchip

Para além da habitual recepção e envio de dados para o *reader,* a antena do *tag* tem como missão retirar energia do sinal recebido para alimentar o *tag*. Esta antena está fisicamente conectada ao *microchip* e pode ter infinitas variações de formato, conforme a aplicação, o espaço disponível, as frequências da portadora entre outros. As dimensões são, em regra, muito maiores que as dimensões do *microchip*, razão pela qual é o tamanho da antena que determina o tamanho da *tag*. Para que as *tags* passivas entrem em funcionamento é necessário, não só que se encontrem na área visível de, pelo menos, uma antena externa, mas também que o *reader* lhe forneça potência suficiente para que esta tenha capacidade de estabelecer comunicação – esta técnica denomina-se de *backscatter*[1]. Podem ser integradas numa panóplia de aplicações, mas, regra geral, naquelas que implicam permanência de operação. Apresentam baixo coeficiente de degradação com as condições climatéricas sendo por isso resistentes ao desgaste. Existem, no entanto possibilidades de afectação do sinal nos casos de aplicações que tenham madeiras, líquidos viscosos e em pequena percentagem água [20]. Na figura 6 são exemplificadas as representações de uma *tag* deste tipo.

[1]Técnica utilizada pelas *tags* passivas RFID em que a iniciativa de estabelecer comunicação terá que partir do interrogador sendo que a potência utilizada por este será reaproveitada para a *tag* enviar informação.

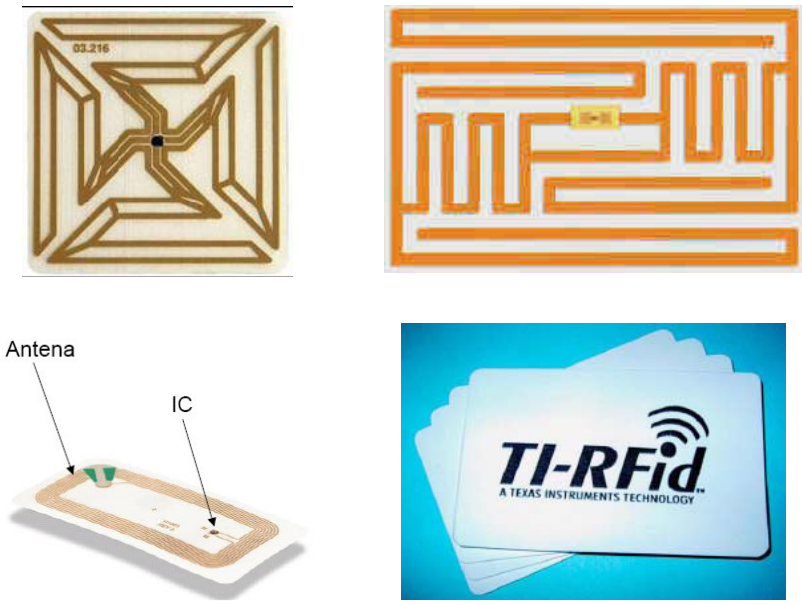


Figura 6 Tags Passivas [2] [39] [40]

Estas *tags* possuem, não só um número identificador, como podem também conter memória não volátil – EEPROM – para armazenamento de dados. Esta característica é somente para as *tags* passivas de Classe 2, pois as anteriores (Classe 0 e 1) dispunham apenas de número de identificação. Possuem ainda tamanhos cada vez menores, devido à ausência de bateria, cifrando-se actualmente com dimensões na ordem da décima de milímetro – e na ordem dos micrómetros de espessura, tendo já em conta o tamanho e desenho da antena embutida nas *tags* (figura 7). Em termos de custos, as *tags* passivas são claramente as menos dispendiosas, podendo ser adquiridas actualmente por somente 0,05 € aproximadamente, dependendo da *tag* em questão, e quando encomendadas em quantidades significativas.

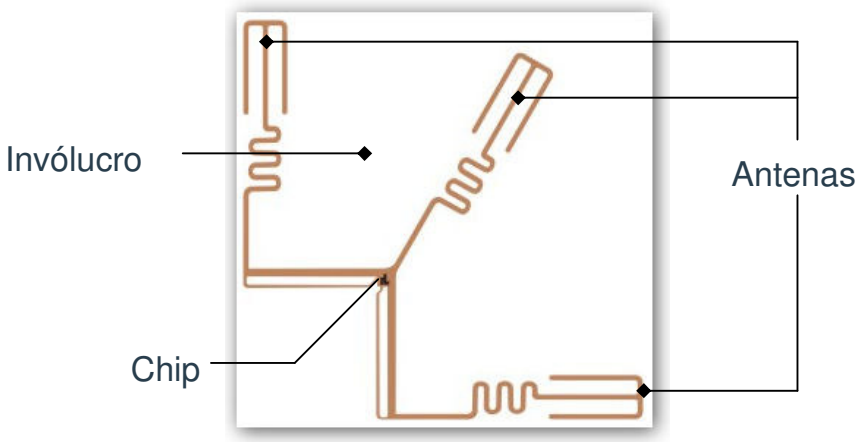


Figura 7 Tag Passiva [33]

Comparativamente às *tags* feitas à base de silicone, existem actualmente alternativas – *tags* feitas de polímero – as quais são menos dispendiosas. De futuro, é tido como objectivo poder imprimir *tags* passivas utilizando uma simples impressora, tornando esta tecnologia praticamente gratuita, à semelhança dos códigos de barras (é apresentada, no capítulo da aplicação, uma destas soluções, porém ainda não disponível à generalidade do público).

2.2.1.2 Tags Activas

As *tags* activas (figura 8) têm uma constituição e aplicabilidade complementar às passivas. Estas possuem uma bateria e um circuito rádio que lhes permite transmitir o próprio sinal para o *reader*, ao invés de dependerem deste para serem alimentadas. A grande vantagem da utilização destas *tags* prende-se, principalmente, com o alcance que estas oferecem – actualmente na ordem das dezenas de metros – abrangendo, desta forma, outro tipo de aplicações dependentes do alcance. O facto de possuir uma bateria permite-lhe estar activa de forma contínua e de necessitar de pouca potência para que possa comunicar com uma antena. No entanto este factor (bateria) limita o tempo de vida útil, sem manutenção, deste tipo de equipamento [4]. Do ponto de vista dos custos por cada *tag*, estes são consideravelmente superiores, pelo que não poderão ser utilizadas para aplicações que impliquem uma eventual inutilização das mesmas. O tamanho destas *tags* é também superior ao das *tags* passivas o que constitui certamente, em alguns casos, um factor negativo. Dispõem ainda de outras funcionalidades, que não existem nas *tags* passivas, fruto de serem auto-alimentadas: podem efectuar monitorização e controlo independente; podem tomar iniciativa no estabelecimento de comunicações; têm capacidade para

executar diagnósticos; possuem largura de faixa superior às alternativas e podem estar equipadas com mecanismos que lhes permitem detectar qual o melhor caminho para comunicar [2].

Figura 8 Exemplos de tags activos [39]

2.2.1.3 Tags Semi-Passivas

Estas *tags* são um híbrido de tecnologias dos dois outros formatos, agrupando algumas vantagens e também desvantagens. Usualmente permitem que se atinjam alcances na ordem das dezenas de metros – como nas *tags* activas – e são igualmente alimentadas.

Figura 9 Tag Semi-Passiva [27]

A principal diferença para com as *tags* activas está relacionada com o facto das semi-passivas não estarem permanentemente activas, ou seja, necessitam de receber um sinal eléctrico proveniente de uma antena para que estabeleçam uma comunicação (utilizam *backscatter*). Além disso são igualmente menos dispendiosas que as *tags* activas [4]. Como tal, para determinado tipo de aplicações, são outra alternativa bastante viável. A referenciada na figura 9 possui uma bateria capaz de durar 30 anos precisamente devido às características explicitadas. Pode responder, armazenar dados e registar eventos como por exemplos as temperaturas a que funcionou, se alguém a desmontou, se existe degradação dos sinais, quais foram dos dados que leu e escreveu e quais os dados lidos e escritos [27].

2.2.1.4 Comparação Activo vs Passivo

Para além das diferenças já referidas nas secções anteriores, pela tabela 5 pode-se ver que as *tags* activas têm maior capacidade de armazenamento, maior rapidez de acesso múltiplo e melhores aplicações em termos de segurança devido à sua capacidade de armazenamento de informação [2]. Contudo, pelo facto de serem mais dispendiosas leva a terem um impacto mais reduzido nos processos de negócio, pois para muitas aplicações as *tags* passivas são suficientes e muito mais baratas.

	RFID Activo	**RFID Passivo**
Bateria	Sim	Não
Potência no Tag	Continua	Só quando ao alcance do Reader
Sinal reader/tag	Fraco/Forte	Forte/Fraco
Alcance	Longo(100 m)	Curto(3 m)
Multi-tag Collection	Milhares em Repouso	Centenas de Repouso
Memoria	Acima de 128 KB	128 bytes
Capacidades	Actualização permanente	Actualização quando perto reader
Monitorização de área	Sim	Não
Velocidade elevada Acesso múltiplo	Sim	Limitada
Aplicações de segurança	Sofisticadas	Básicas
Manifesto electrónico	Sim	Não
Impacto nos processos de negócio	Reduzido	Substancial
Aplicações características	Processos comerciais dinâmicos Segurança e sensibilidade Armazenamento de dados/ "logging"	Processos comerciais fixos Segurança reduzida Fraca capacidade de armazenamento de dados.

Tabela 5 Quadro comparativo entre RFID passivo e activo

Há ainda que se ter em atenção o ambiente em que as *tags* operam. Quando existem líquidos de qualquer natureza ou até humidade existe alguma inoperância ou perturbação no funcionamento destas, principalmente das passivas [20]. Observam-se distorções de sinal a níveis de concentração de água na casa dos 4 g [14]. Já existem antenas que contornam algumas destas questões mas a evolução tem de passar também pelas etiquetas. A solução para contornar este tipo de questões passa por fabricar etiquetas cujo material de que são constituídas possa alterar as suas caracteristicas de dieléctrico de forma mais significativa quando exposta a tais condições de local [10]. Ou então deve ser posta em

execução a etiqueta multi-frequência para associação com as antenas da mesma categoria (explicado em Antenas) [20].

2.2.1.5 Frequência das Tags

Existem alguns padrões de RFID, relativos tanto à tecnologia como à utilização. Os principais são o ISO e a EPCglobal (www.epcglobalinc.org) assim como existem inúmeras faixas nas quais os diversos tipos de *tags* operam, o que é tentado para se explicar aqui é quais são as vantagens de se utilizarem determinadas frequências em detrimento de outras (resumo na tabela 6). Obviamente toda esta análise irá centrar-se nas soluções actualmente disponíveis no mercado e que poderão sofrer alterações de futuro. As operações RFID são dirigidas pelas autoridades locais que controlam o espectro electromagnético [21]. Por exemplo as etiquetas de 915 MHz não podem ser lidas através de alguns materiais, por isso são desaconselháveis para localização de objectos em unidades de fabrico. Se a velocidade de processamento e o espectro da região permitirem, os leitores de 13,56 MHz são os mais apropriados [21]. Nas figuras 10 e 11 podem-se consultar duas representações onde se encontram os espectros divididos por regiões a nível mundial e respectivas características dos mesmos.

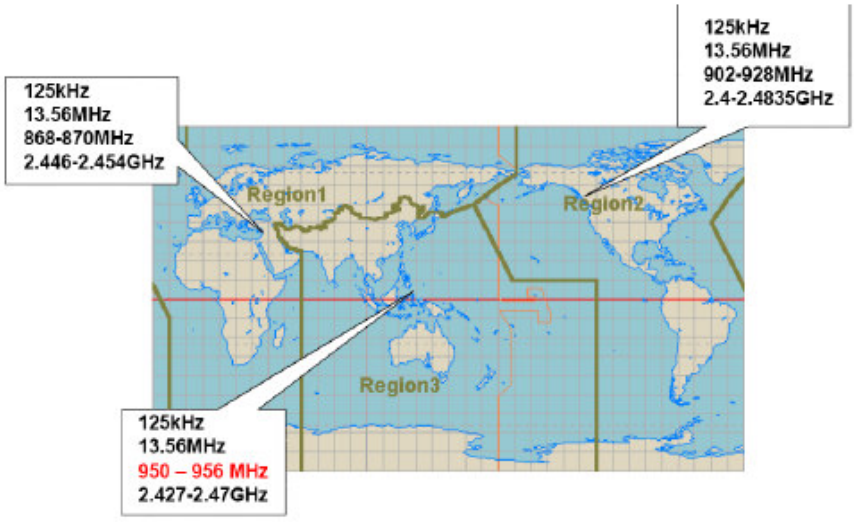


Figura 10 Distribuição do espectro de frequências por regiões

Figura 11 Distribuição do espectro de frequências por continentes [40]

Faixa de frequência	Benefícios	Problemas	Aplicações Típicas
LF 100-500 kHz	• Baixo custo • Melhor penetração por objectos não metálicos	• Baixo a médio alcance de leitura • Velocidade de leitura baixa	• Controlo de acessos • Controlo de inventário
HF 10-15 MHz	• Baixo a médio alcance de leitura • Velocidade de leitura média	• Apresenta custos superiores às da faixa inferior	• Controlo de acessos • *Smart cards*
UHF 850-950 MHz	• Alto alcance de leitura • Velocidade de leitura alta	• É necessária linha de vista • Dispendioso	• Identificação de veículos e sistemas de controlo de entradas
UHF 2,4-5,8 GHz	• Alto alcance de leitura • Velocidade de leitura alta	• É necessária linha de vista • Dispendioso	• Identificação de veículos e sistemas de controlo de entradas • Geração 802.11 de WLAN

Tabela 6 Características dos diversos tipos de frequências [39]

Existe uma grande variedade de frequências de operação possíveis, no entanto há restrições à utilização de algumas em determinados países, sendo que deverá ser consultada a legislação a aplicar consoante o país onde pretendemos implementar a solução.

Banda [MHz]	303 302-305	315 314,7-315	418 418,95-418,975	433 433.05-434.79	868 868,0-868,6	915 902-928	2400 2400-2483.5
EUA	✓	✓	✓	✓		✓	✓
Canadá	✓	✓	✓	✓		✓	✓
Grã-Bretanha				✓	✓		✓
França				✓	✓		✓
Alemanha				✓	✓		✓
Holanda				✓	✓		✓
Singapura		✓		✓	✓	✓	
Taiwan	✓	✓	✓	✓			✓
China Hong Kong				✓		Limitada	Limitada
Austrália				✓		Limitada	Limitada
Sumário	Aceitação limitada	Aceitação limitada	Aceitação limitada	Melhor escolha	*Duty cycle* limitado	Aceitação limitada	Limitação à linha de vista

Tabela 7 Uso de frequências a nível internacional [39]

Da análise que resulta (tabela 7), pode-se desde já concluir que a faixa dos 850 a 950 MHz (UHF) está a ser amplamente utilizada para implementar este tipo de soluções, pelo mundo fora. No entanto não se descartam as restantes, tudo dependerá do tipo de aplicação que se pretende. Igualmente de realçar, possuímos as frequências de microondas – dos 2,4 aos 5,8 GHz – a qual poderá facilitar integração com tecnologias já existentes (/e.g./ IEEE 802.11a/b/g). A faixa dos 433 MHz foi adoptada para as *tags* activas. Obviamente que esta escolha é feita tendo por base as tendências de mercado actuais e regulamentação existente pelo que poderá, de futuro, sofrer alterações. Qualquer uma destas faixas seria viável, quer fossem as mais baixas para sistemas de curto alcance, quer as mais altas, com maior alcance – mas com prejuízo de ter de existir linha de vista. A escolha pelos 433 MHz deve-se à grande aceitação desta frequência mundialmente, a qual se encontra regulamentada e aprovada na maioria dos países. Além disso evita-se a utilização do espectro entre os 862 MHz e os 928 MHz – que é mais utilizado para as *tags* passivas [39].

2.2.1.6 Capacidade de Armazenamento

Dependendo do tipo de *tag*, a quantidade de informação pode variar desde alguns bytes a vários megabytes de informação. Esta pode ser organizada em vários formatos, desde que a *tag* e o *reader* concordem num único formato de funcionamento. Muitos formatos são proprietários, contudo algumas normas começam a emergir.

O *Electronic Product Code (EPC)* é considerado a norma RFID (tabela 8) que virá substituir o (UPC) *Universal Product Code,* usado pelo código de barras. O novo EPC usa

o *General Identifier* (GID-96) da organização EPCglobal. A EPCglobal é uma organização sem fins lucrativos criada pelo *Uniform Code Council* e pelo *European Article Number International* para comercializar a chamada tecnologia de Código de Produto Europeu (EPC) que interliga o RFID com a Internet de forma a permitir uma imediata e automática identificação assim como uma partilha mais ou menos segura de informação na cadeia de troca de acessos [15]. O GID-96 contem 96 bits ou seja 12 B de informação, e esta informação encontra-se organizada em 3 classes.

	Cabeçalho	Empresa	Classe do Objecto	Serial
Número de bits	8	28	24	36
Números possíveis		268.435.455	16.777.215	68.719.476.735

Tabela 8 Norma EPC [39]

A informação organizada desta forma permite que 30 939 155 745 879 204 468 201 375 números únicos sejam criados.

As *tags* possuem memórias e é possível fazer uma divisão da forma como se comportam as memórias destas. Assim sendo, podem-se diferenciar três tipos de memórias geralmente usadas: *Read Only* (RO), *Write Once Read Many* (WORM) e *Read-Write* (RW) [39].

2.2.1.6.1 Read only

Muitas *tags* passivas pertencem a esta categoria. As *tags* RO apenas permitem a leitura dos dados contidos na sua memória. São programadas uma vez na vida, geralmente na própria fábrica (ex: código EPC). Sendo *tags* unicamente de leitura, a sua gravação é permanente, não sendo permitido à *tag* qualquer actualização dos dados. Este tipo de *tags* é prático para pequenas aplicações comerciais ou para fins de localização com etiquetas normalizadas, como, por exemplo, em lojas de roupas ou bibliotecas [2]. No entanto, tornam-se impraticáveis para grandes processos de manufactura ou para sistemas que necessitem de actualização de dados.

2.2.1.6.2 Write Once, Read Many

Em teoria, os *tags* WORM poderiam apenas ser programados uma vez pelo seu comprador no momento e para o fim que necessitasse [2]. No entanto, na prática existe a possibilidade

de reprogramar alguns tipos de *tags* WORM mais que uma vez sendo que os números típicos andam a volta das 100 vezes. Todavia, se o número de reprogramações for elevado, corre-se o risco de danificar permanentemente a *tag,* inutilizando a sua memória. No entanto, esta reprogramação não permite à *tag* a sua auto-actualização, pois esta terá sempre que ser feita por um programador em material indicado para esse fim.

2.2.1.6.3 Read-Write

As *tags* RW são as mais versáteis, pois podem ser reprogramadas inúmeras vezes. Tipicamente, este número varia entre 10 000 e 100 000 vezes, no entanto já existem *tags* onde este limite é muito superior. As vantagens deste tipo de *tags* são imensas quando comparadas com as restantes, pois permitem, a título de exemplo, actualizações permanentes da informação contida na sua memória, elaboração de um histórico do percurso de um produto, monitorização em tempo real da temperatura ou outra variável física, entre muitas outras coisas. Uma *tag* RW tipicamente contém uma memória *Flash* ou FRAM. Este tipo de *tags* é a mais indicada para segurança de dados, monitorização de ambientes e processos que precisem de actualização de dados constante. Obviamente que estas *tags* são mais caras que todas as anteriores e, por esse motivo, ainda não são usadas com grande regularidade.

Identificando cronologicamente (tabela 9) as *tags* mediante o protocolo e as suas capacidades facilmente se distingue cada uma das normas.

Protocolo	Capacidades
EPC Generation 1 – Class 0	"*Read-Only*", pré-programado
EPC Generation 1 – Class 1	"*Write-Once*", "*Read-Many*"
ECP Generation 2.0 Class 1	*"Write-Once", "Read-Many",* versão aceite globalmente.
ISO 18000 Norma	"*Read-Only*", pode conter memória para que dados do utilizador possam ser escritos. Este protocolo é composto por diferentes secções dependendo da frequência usada e da intenção de uso.
ISO 15963	Unique Tag ID
ISO 15961	Protocolos de dados: Regras de codificação dos dados e funções lógicas de memória.
ISO 15962	Protocolos de dados: interface da aplicação.

Tabela 9 Protocolos criados pela EPCglobal e ISO [39]

2.2.2 Readers

Um *reader* (assim chamado devido ao termo anglo-saxónico que significa basicamente o aparelho que permite ler, interpretar e escrever (ao contrário do que faria supor) *tags* RFID. Para tal efeito, o *reader* liga-se a uma ou mais antenas de um qualquer interface definido pelo construtor e usa-as para emitir ondas de rádio, com energia fornecida pelo próprio *reader*. Se uma *tag* activa se encontra no campo de visão (*zone*), esta irá usar a energia para emitir o seu próprio sinal. Esse sinal é então capturado por uma ou mais antenas que o transmitem e o leitor (*reader*), por sua vez, irá traduzir o sinal recebido que contém a informação da *tag*. Permitirá então redireccionar essa informação da maneira que o utilizador quiser. Na figura 12 encontra-se um exemplo de um *Reader*.

Figura 12 *Reader* [33]

Existem vários tipos de *readers*, distinguidos por várias características que vão desde a(s) sua(s) frequência(s) de trabalho até ao seu carácter de mobilidade, passando pelas interfaces de comunicação ou pelo seu *firmware*. A grande maioria dos *readers* lê em todas as frequências usadas pelas *tags*, ou em espectros específicos de determinado tipo de *tag*, mas existem também aqueles que permitem configurar tais parâmetros (para funcionar como filtro, por exemplo), tornando-se também uma característica de *firmware*. Porém a característica mais predominante, e que mais condiciona a escolha dos compradores além do preço, prende-se com a mobilidade. A escolha entre *readers* fixos (figura 12), ou móveis (à semelhança dos emissores de infravermelhos) depende do uso que os compradores querem dar ao equipamento, seja para colocar na entrada de uma plataforma de carga, num empilhador, ou na mão de um funcionário [4].

Para possibilitar a interacção com outros dispositivos, os *readers* são fabricados com várias portas de comunicação: portas de rede (RJ45, *Ethernet*); portas USB e portas de série, além das portas de comunicação com as antenas (normalmente cabo coaxial). Obviamente o

número, disposição e tipo destas portas varia consoante o fabricante e consoante o tipo de *reader*. Dispõem muitas vezes de um LCD que lhes permite identificar as tarefas que estão a ser concretizadas pelo mesmo, para controlo do utilizador (figura 13).

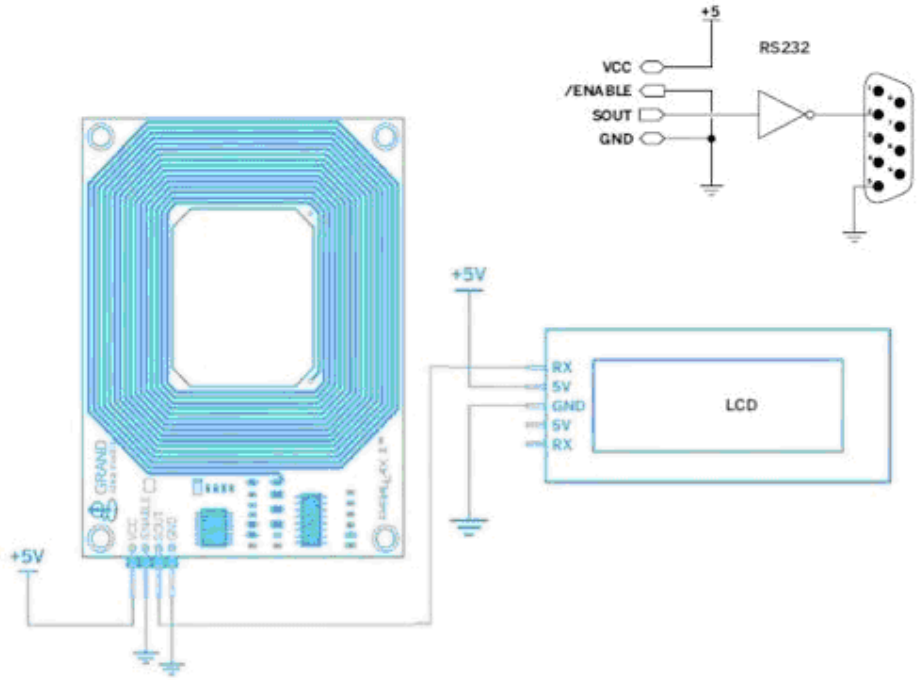


Figura 13 Esquema interno de um Reader

Em alguns casos, o *firmware* dos *readers* é acessível pelo *browser*, num determinado IP, e permite realizar as configurações necessárias para que possa funcionar de acordo com as pretensões do utilizador [2]. Será geralmente tanto melhor, quantas mais configurações permitir efectuar. Dentro destas destacam-se:

- Definições de utilizadores e respectivas permissões;
- Realizar filtros de *tags* (aplicáveis no acto da leitura, ou no acto de envio dos dados para o computador);
- Ler ou escrever informação nas *tags* (tendo em conta que certos *readers* não conseguem escrever em determinado tipo de *tags*);

- Configurações das antenas acopladas e *read points* associados (podem-se definir *read points* para definir portais de antenas, por exemplo para locais de carga e descarga);

- Definir os eventos passíveis de serem detectados (*tag* nova; entrou no campo de visão; saiu; etc.);

- Visualizar *logs*;

- Efectuar controlo de erros e até possibilidade de realizar *updates*, entre muitas outras.

Existem também, e na perspectiva do seu fabrico, *readers* hoje em dia, que mediante a classe de protecção IP65, podem ser montados em exteriores sem ser necessária protecção adicional, que poderia por exemplo limitar o alcance dos mesmos. Estão por isso contempladas também as questões ambientais para este tipo de dispositivo.

Tem existido muita evolução dos preços neste tipo de equipamento. Os *readers*, bastante comuns no mundo do RFID têm sido alvo de diminuição de preços assim como o restante *hardware* deste tipo, incluindo antenas, impressoras e *tags* (com a sua gama de preços associada, claro).

A nível tecnológico é perfeitamente possível hoje em dia termos etiquetas a serem lidas por múltiplos leitores e um leitor a identificar várias etiquetas ao mesmo tempo. Num sistema bem elaborado deve-se fazer a chamada "Distribuição de Carga", ou seja, se um leitor está demasiado sobrecarregado deve-se fazer o tratamento das informações deste por alguns outros que possam estar mais disponíveis, sob risco de todo o sistema ficar afectado em velocidade e em paragens [18]. Estas configurações quase sempre não necessitam de ser feitas fisicamente se todos os leitores estiverem interligados, bastando para isso uma modificação no *middleware* [19].

Os *readers* recentes devem fazer cerca de 1800 leituras por segundo e por isso há ainda a referenciar alguns problemas de leitores quando estes se encontram demasiado próximos uns dos outros, que pode causar colisão de pacotes trocados entre estes e as etiquetas [13]. Actualmente, já se contornam estas questões colocando os leitores a executar as leituras alternadamente (através do envio de uma onda periódica quadrada para o leitor) que

permite que quando um esteja a fazer uma validação, o(s) restante(s) esteja(m) "bloqueado(s)" na fracção temporal correspondente [19]. Pode existir ainda a questão de haver a duplicação de leitura de uma etiqueta num curto espaço de tempo, para isso define-se um intervalo mínimo de leitura dessa mesma etiqueta para que esta não possa ser lida em períodos inferiores a este [18].

2.2.3 Antenas

Outra parte fundamental destes sistemas traduz-se nas antenas. Tal como já foi referido, são elas que fazem a interligação entre os *readers* e as *tags*, possibilitando a comunicação entre ambos. Normalmente são alimentadas pelo próprio *reader*, mas podem ter alimentação própria [4].

Alguns dos vários tipos de antena são apresentados na figura 14.

Figura 14 Tipos de antenas [39]
A – Antena de *desktop* ou parede; B – Antena de HF; C – Antenas em portal

Cada antena destina-se, obviamente, a um dado uso. As antenas de *desktop* ou de parede são as mais comuns, satisfazendo a maioria das necessidades, uma vez que (à semelhança de qualquer outra) também se podem agrupar podendo fazer as vezes de antenas de portal (grupo de antenas). O que distingue grandemente as antenas é o seu diagrama de radiação que influencia bastante a eficiência da antena, dependendo do seu modo de utilização. As antenas tipo *desktop* ou de parede possuem um diagrama de radiação lobular como aqueles apresentados na figura 15, dependendo da polarização usada. É claro que estes são modelos teóricos e na realidade nunca são tão perfeitos, mas constituem uma aproximação

razoável. Não será demais obviar que as antenas apenas capturam aquilo que estiver no interior dos lóbulos [2] [4].

Sistemas desenvolvidos têm demonstrado que a presença de antenas em quantidade fazem reforço do sinal e por isso criam maior facilidade de identificação do objecto nomeadamente no que diz respeito a alcance e a sensibilidade de orientação [22]. Existem ainda as chamadas antenas de multi-frequência. São elementarmente dispositivos que funcionam a duas frequências distintas localizadas na zona de HF (13,56 MHz) e UHF (800-960 MHz). Como já foi dito, regra geral, um leitor UHF oferece um melhor alcance de leitura e um HF tem vantagens no caso de leituras feitas com líquidos à mistura [11]. Uma utilização dos dois no mesmo sistema revela-se uma solução quase perfeita, pois assim respondem em ambas as faixas. Só ainda não temos no mercado as etiquetas multi-frequência bastante desenvolvidas, mas esse será concerteza um dos pontos a rever.

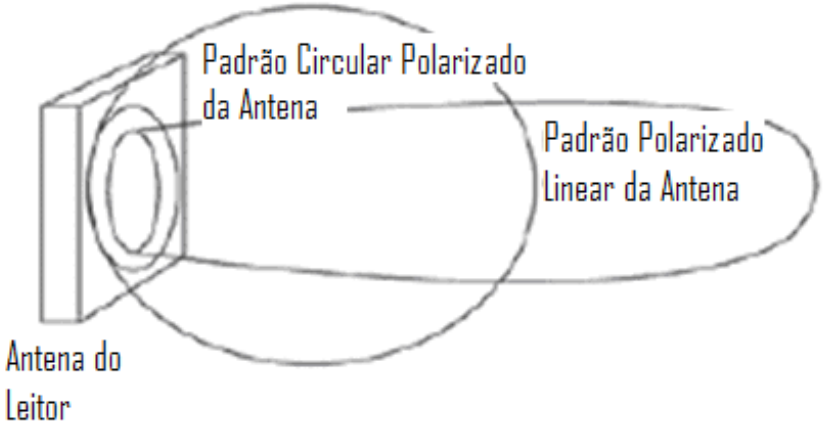


Figura 15 Lóbulos das antenas com polarização linear e circular [39]

Os *readers* possuem as suas próprias antenas incorporadas, normalmente bastante directivas (no sentido da aproximação do objecto), mas dependem das patentes do próprio fabricante, podendo por isso variar bastante de *reader* para *reader* [4].

Existem já, sistemas que podem ser programados para funcionar em diferentes normas como a ANSI e a ISO. Os próprios dispositivos adaptam-se a nível programacional à etiqueta que estiver a ser identificada e fazem por si só a interpretação do código.

2.2.4 Middleware

Na ligação que existe entre o sistema computacional e o módulo RF/Leitor temos o patamar de *middleware*. É a ligação orgânica entre a camada de comunicação do *reader* e a camada de aplicação/*software* [31]. Este sistema valida os dados e, normalmente, usa a *Physical Markup Language* para estruturar a mensagem. Este mais não é do que o tratamento feito aos dados recebidos das etiquetas, através das antenas e do(s) leitor(es) que existam no sistema. Existem alguns protocolos (comunicação) mais usuais e até alguns próprios para este patamar. Os mais usuais são os RS-232 e o RS-485, no entanto o mais conhecido é o *Wiegand* (no entanto este necessita posteriormente de um controlador que converta para um dos dois referidos anteriormente) , que se começou a vulgarizar nos anos 80. Este método de transmissão utiliza dois condutores de dados (*data1* and *data0*) e os cartões de dados utilizam um formato a 16-bit. Devido ao seu alargado uso na época citada, quase todos os sistemas de controlo de acesso permitem o uso de leitores que utilizam esta interface assim como para os formatos dos dados das etiquetas. Sendo assim, temos de ter compatibilização entre leitor, etiqueta e formato dos dados comunicados para que seja válida a norma.

Para que haja compatibilidade eléctrica, todos os periféricos devem ser compatíveis a nível de protocolo e em consequência de controlador. A maior parte dos controladores existentes foram concebidos para aceitar a norma *wiegand*. Isto significa que se quisermos ligar outro tipo de protocolo temos de encontrar um que seja electricamente compatível com o controlador.

Quanto às linhas de sinal a *data1* transporta os bits “1” para o controlador e o *data0* os bits “0”. A figura 16 é uma representação gráfica de uma trama de dados para o valor binário "01101". Cada mudança de estado representa a comunicação de um bit.

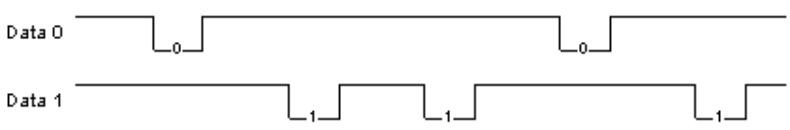


Figura 16 Transmissão em Wiegand

O formato de dados *Wiegand* caracteriza-se pela contagem total de bits e pela distribuição dos campos de dados. A figura 17 mostra o uso dos 26-bit. Consistem em ter um bit de

paridade, 8 bits de código de uso e 16 bits de identificação de utilizador com mais um bit de paridade, o que perfaz os 26 bits.

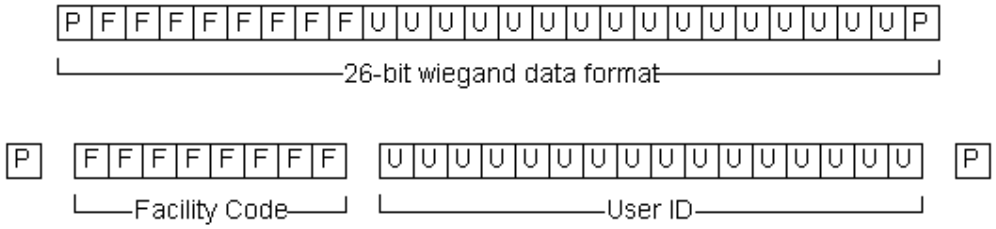


Figura 17 Formato dos dados em Wiegand

2.3 PRINCÍPIOS DE OPERAÇÃO

O funcionamento da transmissão de dados, ocorre a partir da entrada do objecto ou produto contendo a etiqueta inteligente, na área coberta pelo leitor, que emite as suas ondas constantemente. A partir da identificação da etiqueta, o leitor envia um sinal electromagnético, que é recebido pela antena da etiqueta. No retorno da comunicação, a etiqueta transmite um sinal modulado ao leitor com as informações armazenadas. A comunicação entre o leitor e a etiqueta passiva, é realizada utilizando um dos dois métodos existentes para modular o sinal de identificação, que são: baixa frequência, com menos de 100 MHz, ou de alta-frequência que é superior a 100 MHz. O funcionamento da identificação por rádio frequência dá-se a partir de um campo electromagnético, formado entre antenas e algo para responder ao estímulo criado pelo campo magnético, conforme demonstrado na figura 18.

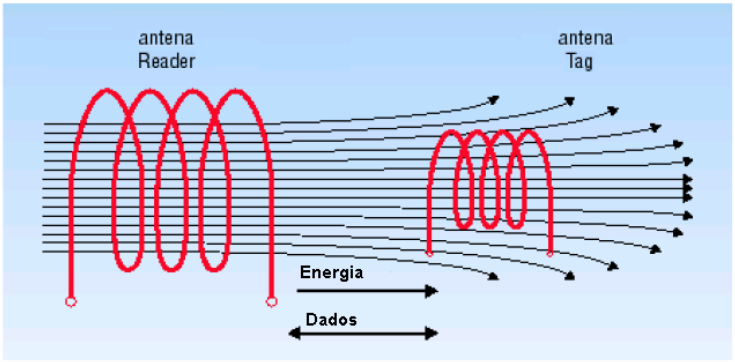


Figura 18 Operação do RFID [37]

Os dados que a etiqueta envia ao leitor, podem conter informação de identificação, de localização geográfica e de especificação do produto que está a servir (preço, data de compra, etc) (figura 19) [5] [7].

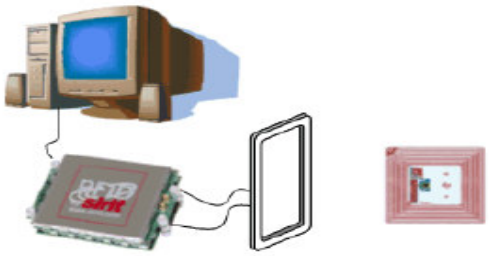


Figura 19 Estrutura típica de um sistema RFID

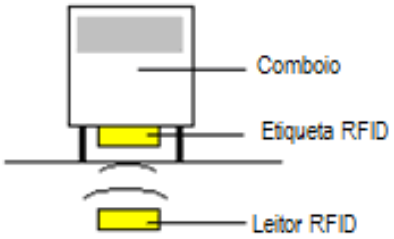


Figura 20 Exemplo aplicação RFID

O leitor ao receber dados da etiqueta, descodifica e reencaminha a mensagem para um sistema anfitrião (*middleware)*. Sempre com o objectivo de identificar objectos, procura-se implementar a tecnologia em várias situações. No meio dos transportes ferroviários (figura 20), a tecnologia é usada para controlar os comboios em movimento e o funcionamento dos sinais assim como das cancelas nas passagens de nível (figura 21) [9].

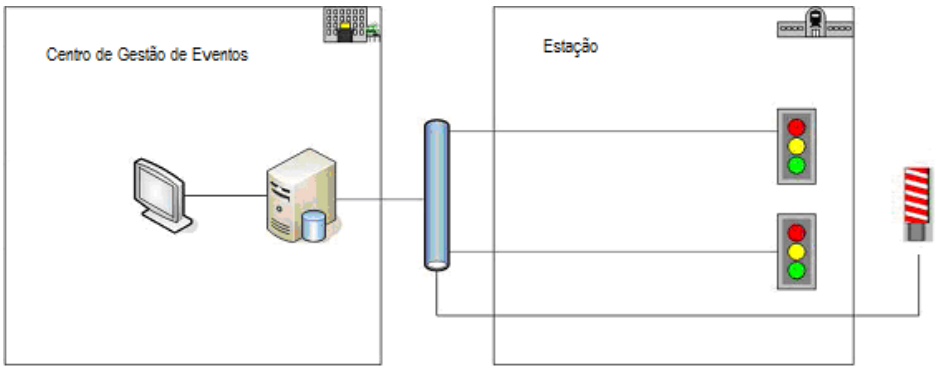


Figura 21 Exemplo Passagens Nível

Os sinais emitidos pela arquitectura RFID, devido à identificação do comboio, passam primeiramente pela estação e são reencaminhados para a central. A central trata o evento e, se for preciso, são enviados comandos para a estação de forma a alterar o estado dos vários dispositivos mecânicos a que tem acesso [5] [7].

A figura 22 exemplifica a arquitectura típica de um destes sistemas.

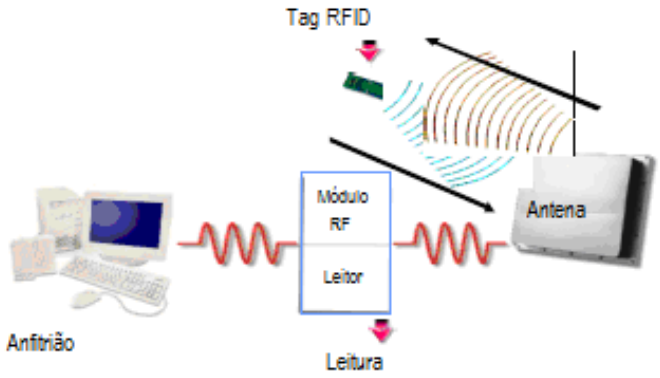


Figura 22 Organização Típica de um Sistema de validação

Os *tags* usam um *microchip* de silício que guarda um número único (*Electronic Product Code* - EPC), e inclui um número de série e informação adicional subdividido em classes conforme refere a figura 23.

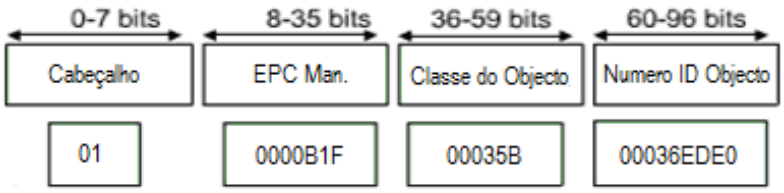


Figura 23 Estrutura do Número EPC

O EPC funciona como uma URL (*Uniform Resource Location*), que é um endereço único para cada produto. Ao ser interrogado pelo leitor, uma vez que esteja sob influência do campo magnético, um sistema conhecido como ONS (*Object Naming Service*), mapeia a informação na etiqueta e envia a mesma para o computador [16]. Há ainda o EPC-*Information Service* (EPC-IS) e o EPC-*Discovery Service* (EPC-DS), dados de informação da EPC. O ONS funciona da mesma forma que o DNS (*Domain Name Service*) na Internet, sendo este o responsável em mostrar para o sistema onde estão as informações necessárias, e como ele deve fazer para ler ou gravar as informações. Na prática, o que ocorre é que qualquer objecto dentro do raio de alcance do leitor que possuir um EPC, o ONS irá efectuar a leitura dos dados da etiqueta. A linguagem utilizada (PML) tem na internet uma linguagem similar, que é o XML (*eXtensible Markup Language*) [37]. A linguagem PML normal é a interacção entre produtos físicos e sistemas, ou seja, é um código padronizado

como o código de barras, com características que permitem o desenvolvimento de software com duas classes, para atender aos diversos tipos de aplicações [16]. São estas:

• EPC classe 0 com 96 bits exclusivamente para leitura;

• EPC classe 1 com 256 bits para leitura e gravação.

Quanto ao EPC-IS este é uma espécie de base de dados acessível publicamente que contem informação dos objectos como por exemplo preço e peso. A informação do EPC-IS é partilhada entre os subscritores e as empresas, e esses dados podem ser alterados precisamente por alteração deste EPC-IS.

Quando um objecto transita de um EPC-IS para outro EPC-IS, dá-se um registo na EPC-DS que regista o historial dos objectos dos subscritores [16].

2.3.1 TIPO DE COMUNICAÇÃO

Até agora têm sido sempre considerados sistemas RFID a funcionar por meio da propagação de ondas de radiofrequência. A esse processo de comunicação, através de um sinal wireless entre o *tag* e o *reader,* dá-se o nome de acoplamento.

Na realidade existem três grandes tipos de acoplamento nos sistemas RFID (figura 24):

1 - Acoplamento indutivo, também designado por aproximação electromagnética
2 - Acoplamento de propagação ou por radiofrequência
3 - Acoplamento por ondas acústicas de superfície

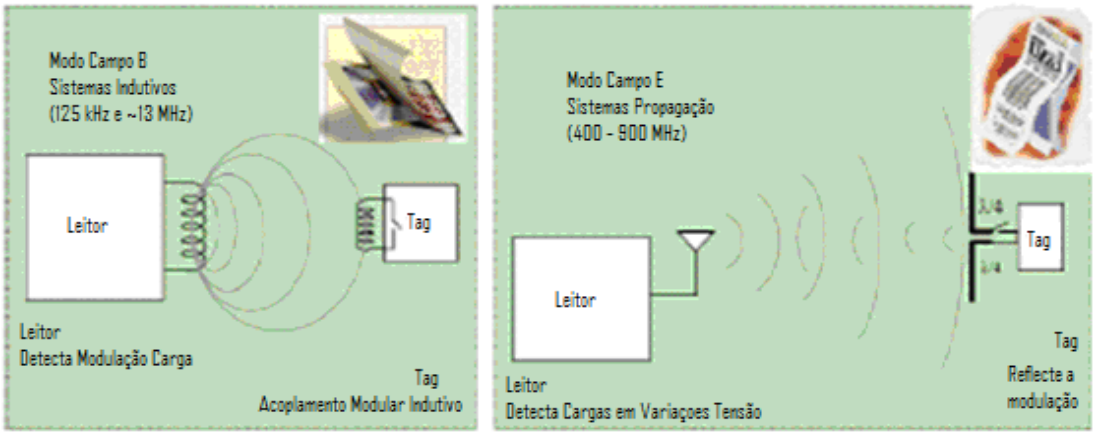


Figura 24 Tipos de comunicação de um sistema RFID

Nos sistemas de acoplamento indutivo (figura 24 - lado esquerdo) a comunicação é feita através da alteração (modulação) dos campos electromagnéticos em torno das antenas. Este tipo de comunicação é muito simples e baseia-se no princípio de ressonância dos circuitos LC. O *reader* gera um campo magnético alternado com uma determinada gama de frequências. Se a frequência de ressonância do circuito LC estiver dentro dessa gama de frequências, existirá passagem de energia do *reader* para o circuito ressonante através da sua indutância.

Nos sistemas de acoplamento de propagação (figura 24 - lado direito) existe a modulação de um sinal RF, que é transmitido entre as antenas dos dois terminais, como num vulgar sistema de rádio. A forma de retorno da informação do *tag* para o *reader* é que varia consoante o tipo de *tag* que se está usar, do meio circundante envolvido, entre outros factores.

Os sistemas de acoplamento por ondas acústicas de superfície baseiam o princípio de comunicação na dispersão superficial das ondas acústicas a baixa velocidade, bem como no efeito piezo-eléctrico (conversão sinal electromagnético em ondas acústicas) [2]. Dentro do substrato piezo-eléctrico existe um transdutor electro-acústico (*interdigital transducer*) e superficies de reflexão, criados com eléctrodos planares. Quando um impulso interrogador de alta-frequência proveniente do *reader* é captado pelo dipólo do *tag*, este é convertido pelo transdutor numa onda acústica de superfície, que se espalha longitudinalmente no substrato. A frequência da onda de superfície corresponde à frequência do impulso proveniente do *reader*. Parte da onda de superfície criada é devolvida aos reflectores, enquanto a restante onda deriva até ao fim do substrato, onde é absorvida. As partes reflectidas retornam ao transdutor, que as reconverte numa sequência de impulsos de alta-frequência, reenviando-a ao *reader*. O número de impulsos da sequência está directamente associado ao número de reflectores existentes dentro do *tag*. O princípio básico do funcionamento está esquematizado na figura 25.

Os *tags* com funcionamento por acoplamento indutivo trabalham nas baixas frequências, enquanto que os *tags* com acoplamento por radiofrequência e por onda acústica de superfície trabalham nas gamas de UHF e microondas [2].

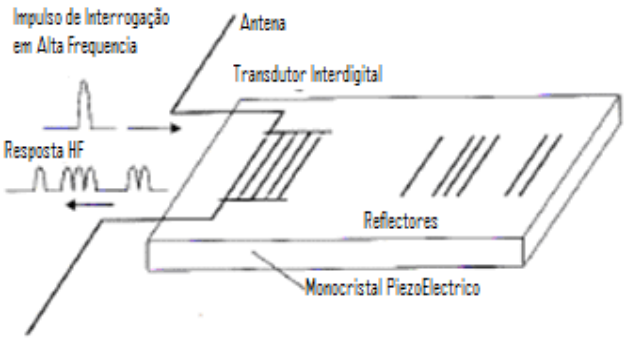


Figura 25 Princípio de funcionamento de um sistema RFID "Dente-de-Serra"(Exemplo)

2.3.2 DIRECTIVAS DE FUNCIONAMENTO

Existem vários princípios de funcionamento de sistemas RFID, como se pode observar na figura 26.

Os sistemas são agrupados em duas classes principais:

- 1 bit Transponder
- N bits Transponding

No entanto, em termos de generalização as subdivisões mais importantes são:

- 1 bit Transponder
- Full and Half Duplex (incluido em N bits)

No grupo do *1-bit Transponder,* o princípio de funcionamento baseia-se na transmissão de apenas um bit ou uma sequência, de informação entre o *tag* e o *reader* (e/ou vice-versa), terminando de seguida a comunicação [2].
Neste grupo, cabem desde os sistemas tipo *On-Off*, típicos em sistemas de alarme de lojas comerciais ou sensores de movimento, até sistemas de permissão de acesso ou leitura de informação armazenada num *smart card* (*tag* em forma de cartão), por exemplo. Este tipo de funcionamento caracteriza-se por ser geralmente rápido e descontínuo, pois exige apenas uma resposta do *tag* para o *reader*. Os *tags* pertencentes a este grupo não têm

necessidade de grandes quantidades de informação nem electrónica complexa para o seu normal funcionamento.

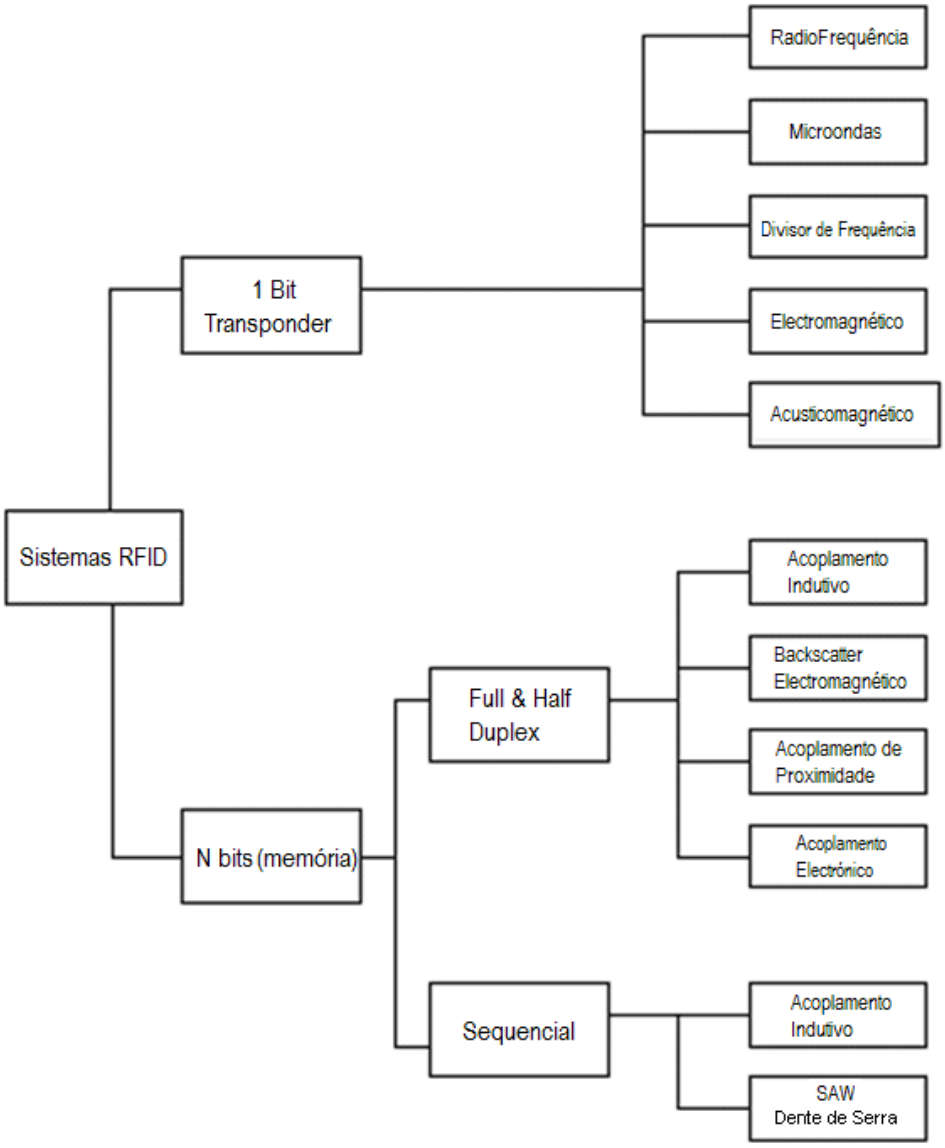


Figura 26 Principais tipos de comunicação em sistemas de RFID

No segundo grupo, o nível de transmissão de dados já é mais complexo, podendo envolver grandes quantidades de informação, em permanente comunicação. Para estes casos, poderá ser necessária a existência de processos e mecanismos de controlo do fluxo de dados entre o *tag* e *reader*. Este é o tipo de funcionamento mais indicado para *tags* com fins de

localização, pois pretende-se obter uma constante monitorização do deslocamento do *tag*, dentro de uma determinada área de cobertura do *reader*.

Dentro deste princípio de funcionamento, podem-se distinguir três formatos diferentes de comunicação (figura 27):

– Full Duplex (FDX)
– Half Duplex (HDX)
– Sequencial (SEQ)

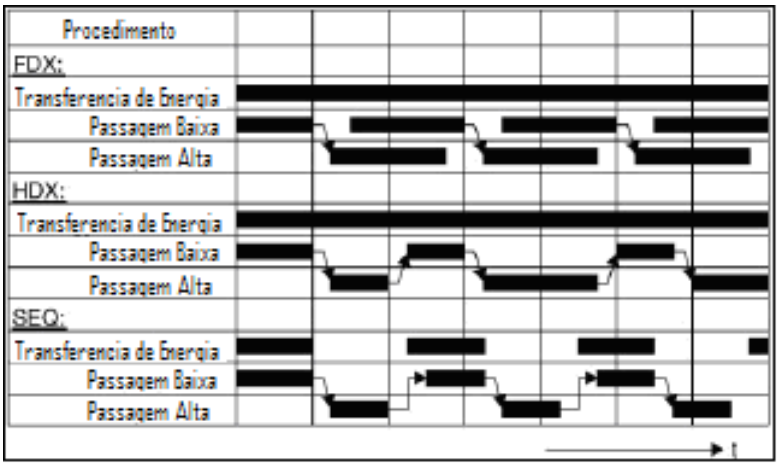


Figura 27 Exemplo comparativo das diferenças de modos de operação

Em *full duplex*, tanto o *reader* como o *tag* estão a transmitir em simultâneo, havendo passagem de dados nos dois sentidos. Isto implica, a existência de um *transceiver* completo no *tag*, para que a comunicação possa ser feita em frequências distintas. Obviamente, caso se esteja na presença de *tags* passivos, a transferência de potência (do *reader* para o *tag*) terá que ser contínua.
Em *half-duplex*, a transmissão de dados do *reader* para o *tag* e vice-versa é feita de modo alternado, ou seja, transmite um de cada vez. Isto permite uma grande simplificação da electrónica envolvida. No entanto, num sistema a funcionar com *tags* passivos, apesar de não estar constantemente a enviar dados, o *reader* terá que enviar um sinal contínuo para alimentar o *tag*, pois este requer energia contínua para o seu correcto funcionamento.

O modo sequencial é parecido com o *half-duplex*. A diferença reside no facto de que agora o *reader* não emite um sinal contínuo de energia mas apenas quando envia dados. O *tag* tem mecanismos de "armazenamento" de energia e utiliza-a apenas na transmissão.

2.3.3 PROTOCOLOS, NORMAS E FABRICANTES

Devido à dispersão de sistemas desenvolvidos e às variadas faixas de frequência usadas em todo o mundo, a criação de protocolos e normas que regulamentassem os sistemas RFID era uma tarefa muito complicada, sobretudo enquanto não fosse encontrado consenso entre os grandes fabricantes de sistemas RFID [2]. Os primeiros protocolos só surgiram na década de 90, com a difusão exponencial dos sistemas protocolos (tabela 10).

	Espectro Frequência				
	LF 125/135 kHz	**HF 14 MhZ**	**HF 433 MHz**	**UHF 900 MHz**	**UHF 2.45 GHz**
ISO	ISO 11784 ISO/IEC 18000-2A	ISO/IEC 14443 ISO/IEC 15693 ISO 18000-3	ISO 18000-7	ISO 18000-6A ISO 18000-6B	ISO 18000-4 ISO/IEC 24370-2
EPCglobal				Class 0 Class 1 Class 1 Gen 2	

Tabela 10 Classificação dos espectros de frequência segundo as normas [40]

2.3.3.1 EVOLUÇÃO DE GERAÇÃO DO PROTOCOLO EPCGLOBAL

Na tabela 11 que se apresenta pode-se verificar a evolução das *tags* da norma EPCglobal. A ideia é que esta evolução seja uma repercussão de uma memória de utilizador cada vez mais alargada, que o espaço reservado ao número EPC seja também ele maior, que as *tags* possam ter identificadores próprios (números de série) cada vez mais precisos e que possuam também protecções ao nível dos roubos, das leituras indevidas e comandos de calibração. Existem ainda especificidades que podem ser melhoradas como por exemplo o alargamento das frequências de operação e das temperaturas de funcionamento.

Característica	Class 1 Gen 2	Class 1 Gen 1
Velocidade de leitura por segundo	**Até 880 (US FCC)** Até **450 (EU ETSI)** Velocidade adaptável ao ruído em RF	**Até 230 (US FCC)** Até **115 (EU ETSI)**
Velocidade Escrita (EPC a 96 bit)	Mínimo de 5 b/s Múltiplas Regravações	3 b/s Múltiplas Regravações
Protocolo TAG	Protocolo**"Q": permite um algoritmo com 2 estados simétricos (o que activa a contagem com múltiplas Tags para o mesmo EPC)**	Algoritmo em ramificação binária com estados persistentes de activação e desactivação
Verificação Dados TAG	**16-bit CRC para leituras e escritas**	**16-bit CRC para leituras**
Operação com múltiplos *Readers*	**Comutação frequência (USFCC)** **Escuta antes de escrita (EUCEPT)** Modos de leitura mais densos (selecção de canal, modulação de portadoras variáveis) **Múltiplas (4) sessões de leitura que permite comunicação paralela com múltiplos leitores para uma só Tag**	Comutação Frequência **(US FCC)** **Escuta antes de escrita (EU CEPT)**
Segurança	Passwords de bloqueio e anulação a **32-bit** Opção para manipulação de comunicação	Password de anulação e bloqueio a **8-bit depois de consecutivas tentativas**
Extensibilidade	**Até 512 e 96 bits de itens** Memória de utilizador ilimitada Antecipa os sistemas de Classe 2 & 3	Até **96 bits de itens**

Tabela 11 Diferenças de características entre gerações da norma EPCglobal [40]

A ideia fulcral de produção de uma *tag* reside na grande necessidade de ter baixo custo, baixa latência, com grandes potenciais de leitura que sejam feitos de forma independente em relação a *tags* que estejam próximas [29]. A primeira geração de *tags* EPC (conforme se pode verificar na tabela) sofria de problemas de falta de recursos computacionais para grandes autenticações encriptadas. Receptoras de sinal dado pelo *reader*, estas não possuíam clocks internos e não conseguiam distinguir diferentes modos de operação mediante o *reader* que encontrassem. Já a geração 2 veio complementar todas as falhas da sua predecessora e introduziu ainda novos factores como *passwords* encriptadas de tamanhos significativos.

2.4 COMPARAÇÃO DO RFID COM O CÓDIGO DE BARRAS

A tecnologia mais óbvia, que é comparável a RFID para muitas áreas de aplicação, é o código de barras. Ambas envolvem uma identificação através de etiquetas, que contém informações que permitem ser identificadas por um computador [37]. Um sistema projectado para identificar objectos em etiqueta de RFID, tem inúmeras vantagens sobre o sistema de código de barras convencional:

- A etiqueta de RFID pode ser reaproveitada e a etiqueta de código de barras uma vez definida, é impressa e fixada uma única vez no objecto ou produto que se deseja identificar;

- A amplitude para leitura do RFID é maior do que a do código de barras;

- Com a etiqueta de RFID, é possível detectar o item em armazenamento para verificar o tempo de armazenamento, ou associar a informação ao processo de fabrico. Isto não é possível com a utilização do código de barras;

- A etiqueta de RFID permite actualizar informações no armazém com os artigos em movimento, mantendo informações importantes na etiqueta e nos sistemas de informações, disponibilizando-as a qualquer ponto de consulta electrónica;

- Os códigos de barras têm que ser "lidos" através de *scanners*, deliberadamente por uma pessoa, sendo difícil automatizar esta acção. Por outro lado, a utilização de RFID permite a leitura através dos *scanners*, sem envolvimento humano, com a obtenção dos dados continuamente, o que significa leituras menos caras e mais precisas;

- A etiqueta de RFID pode ser lida em grande quantidade, simultaneamente, enviando os dados para um computador, ao invés de leitura individual como exige o código de barras;

- A etiqueta de código de barras exige uma linha de visão, enquanto a etiqueta de RFID, pode ser lida desde que esteja dentro da amplitude de radiofrequência dos leitores em qualquer direcção;

- Os leitores de RFID podem comunicar-se simultaneamente com múltiplas etiquetas inteligentes, em razão da capacidade do leitor para capturar o conteúdo de uma remessa inteira, identificando a localização no armazém ou nos recipientes de transportes, com capacidade de seleccionar detalhes das informações numa passagem, sem a necessidade de interromper o fluxo da movimentação dos produtos;

- A etiqueta de Código de barras, não trabalha quando exposta a elementos líquidos, corrosivos, sujos, que danificam ou interferem de qualquer forma o material da etiqueta;

- A etiqueta de RFID recebe as informações que devem conter na etiqueta, e podem ser alteradas e modificadas, permitindo inúmeros controlos tais como o tempo de armazenamento, leitura clara fora da linha de visão, inclusive em ambientes severos;

- A etiqueta inteligente pode armazenar mais dados que o código de barras, significando grande vantagem no processo de armazenamento e movimentação dos produtos na cadeia logística [37].

Além da tecnologia de RFID, e sistemas de controlo através de etiqueta com código de barras, há também inúmeras tecnologias que podem ser utilizadas de modos semelhantes, para armazenar informações ou identificar objectos. Estas tecnologias incluem banda magnética e sistemas de contacto, para armazenamento das informações em sistemas computacionais [37].

Na tabela 12 demonstram-se resumidamente as principais características de algumas tecnologias das etiquetas de identificação.

Características	Tecnologia das Células			
	RFID Passivo	Código de Barras	Faixa Magnética	Memória de Contacto
Capacidade de Dados	Alta	Média	Baixa	Alta
Visibilidade Humana	Invisível	Visível	Visível	Visível
Identificação Simultânea	Sim	Não	Não	Não
Robustez	Alta	Baixa	Média	Média
Distancia para Operação	Alta	Média	Baixa	Baixa
Exige Contacto Directo?	Não	Sim	Não	Sim
Problemas com Objecto Metálico	Sim	Não	Sim	Sim
Custo do Leitor	Alto	Médio	Baixo	Baixo

Tabela 12 Diferenças entre tecnologias de identificação [37]

Considerando a utilização da tecnologia de etiqueta inteligente na cadeia logística, apresentam-se como evidentes, as vantagens da tecnologia de RFID, sobre as demais que foram comparadas. A leitura sem a visibilidade humana, bem como a identificação simultânea de diversos produtos, são características disponíveis na tecnologia de RFID, e de vital importância na movimentação de produtos. Tome-se como exemplo o caso das lâminas de barbear. Com códigos de barras conseguimos identificar que o produto é de facto uma lâmina de barbear, mas com RFID podemos ir ao pormenor de ver se é a primeira, segunda, terceira ou subsequentes lâminas de barbear de uma determinada prateleira de um qualquer local de consumo [26]. Portanto apesar dos investimentos exigidos para a implementação da tecnologia RFID, os resultados e as vantagens evidenciadas, justificam o projecto que assegura melhorias consideráveis nos processos, precisão nos inventários, e consequentemente a redução de mão-de-obra e dos custos inerentes a automatização [37].

3. SEGURANÇA E FUTURO

A decisão por uma determinada tecnologia implica o conhecimento de uma série de parâmetros e para isso temos de fazer um enquadramento. Conhecidos que são os códigos de barras, torna-se pertinente saber quais são as possibilidades de integração do RFID. Na sequência apresentam-se aquelas que serão algumas das vantagens e desvantagens do RFID face a dispositivos de aplicações semelhantes [28]. Alguns dos motivos que levam as empresas a apostar no RFID são (relativamente a tecnologias similares):

• Segurança acrescida – 63%

• Visibilidade dos bens acrescida – 50%

• Aumento da velocidade de operação – 39%

• Aumento da integridade dos dados – 37%

• Redução dos custos de operação – 36%

• Redução dos custos de inventário – 35%

• Aumento da Distribuiçao de Produtividade – 40%

• Melhoria Produtividade dos Pontos de Venda e Retalho – 20%

• Redução das Peças sem armazenamento – 50% [28]

3.1 VANTAGENS

- Capacidade de armazenamento, leitura e envio dos dados para etiquetas activas (móveis);

- Detecção sem necessidade da proximidade da antena para o reconhecimento dos dados - Permite que as *tags* sejam lidas de distâncias consideráveis e a alta velocidade (este parâmetro torna-se particularmente importante quando há a necessidade de identificação de peças a alta velocidade como por exemplo num tapete rolante) [29].

- Durabilidade das etiquetas com possibilidade de reutilização [38];

- Dado que não existe necessidade de as *tags* serem visíveis, estas podem ser integradas em materiais rugosos protegidas de ambientes menos aconselháveis - Por exemplo a integração destas em fluidos corrosivos, ambientes de químicos perigosos e situações de manipulação complicada ou ainda locais de fogo, gelo, com gordura, com ruído ou temperaturas oscilantes [36];

- Número elevado de itens em simultâneo - O que não acontece com materiais que tem de ser lidos/escritos em "linha de visão" (código de barras) [38];

- Exclusividade das *tags* - integração de número de série que é único em todo o mundo;

- *Tags* activas que podem ser programadas - Emitindo ou recebendo informação que seja útil num determinado contexto. [37]

3.2 DESVANTAGENS

- Custo elevado da tecnologia RFID em relação ao código de barras - Actualmente, uma etiqueta inteligente custa nos EUA cerca de 0,05 € cada, na compra de mil

chips. No resto do mundo, esse custo sobe para 0,15 € até 1 € a unidade, dependendo da *tag* em utilização;

- Preço final dos produtos - A tecnologia não se limita ao *microchip* anexado ao produto pois na estrutura estão antenas, ferramentas de filtragem das informações e sistemas de comunicação, mas isso também nos códigos de barras existe, embora a custos mais reduzidos;

- O uso em materiais metálicos e condutores relativos ao alcance de transmissão das antenas - Como a operação é baseada em campos magnéticos, o metal pode interferir negativamente no desempenho. Entretanto, encapsulamentos especiais podem contornar esse problema. Mesmo assim, o alcance das antenas depende da tecnologia e frequência usadas, podendo variar de poucos centímetros a alguns metros (cerca de 30 m), dependendo da existência ou não de barreiras;

- A padronização das frequências utilizadas - Para que os produtos possam ser lidos por toda a indústria, de maneira uniforme;

- A invasão da privacidade dos consumidores - Por causa da monitorização das etiquetas coladas nos produtos e a própria captação de sinais de radiofrequência na vizinhança do sistema. Existem técnicas de alto custo que, quando o consumidor sai fisicamente de uma loja, a funcionalidade do RFID é automaticamente bloqueada.

3.3 SEGURANÇA NO RFID

Já foi visto até este ponto como o RFID funciona na teoria. Nesta parte da tese aborda-se como implementar a segurança no RFID e alguns possíveis ataques, assim como os mais comuns. Antes da análise dos tipos de possíveis ataques, temos de em primeiro lugar analisar quais são os potenciais alvos sujeitos a ataques. O alvo pode ser o sistema na sua totalidade (se o objecto for a destruição completa da solução de negócio), ou pode ser apenas a destruição parcial do sistema (desde a destruição de uma base de dados a um item) [31].

Considere-se o seguinte exemplo num sector de retalho: Se uma *tag* RFID fosse manipulada para que o preço do bem passasse de 200 € a custar 19.95 € no ponto de venda,

neste caso a loja iria ter um prejuízo de 90% sem que os dados da base de dados fossem alterados.

3.3.1 OBJECTIVOS DO HACKER

Antes de se determinar o tipo de ataque, devemos em primeiro lugar tentar perceber qual o objectivo deste, o que irá ajudar a apurar a natureza. Quando um hacker efectua um ataque a um sistema RFID pode ter vários objectivos, desde roubar um simples bem, a impedir que uma loja ou uma cadeia de lojas consiga vender os seus próprios bens. Um atacante pode alterar a informação contida na base de dados para que a informação deixe de ter qualquer valor. Porque existem vários componentes num sistema RFID, existem também vários métodos (ou vectores) usados para atacar o sistema. Os vectores vão de ataques "no-ar", a manipulação da informação das *tags*, manipulação da informação proveniente do *middleware*, e ataque à base de dados ou ainda ataques ao *backend* [39].

3.3.2 MANIPULAÇÃO POR RÁDIO FREQUÊNCIA

Um dos ataques mais simples de executar é o de impedir que a *tag* seja lida pela antena, para isso basta apenas que a *tag* seja coberta por uma folha de alumínio ou num saco de poliéster e revestido por um material metálico. Este método é tão eficaz que pretende-se usar para proteger de ataques que possam ser feitos através do ar. As *tags* e os *readers* são vistos como uma entidade, mesmo que efectuem funções diversas. Um ataque através do ar (ou *attack-over-the-air-interface*) é tipicamente caracterizado por: *Spoofing*, *Insert*, *Replay* e ataques *Denial of Service* (DoS). Um outro método de manipulação tira partido da dificuldade que alguns leitores possuem de não interpretar bem a identificação quando existem muitos sinais a serem processados em simultâneo. Esta situação pode criar situações embaraçosas pois pode registar só algumas das passagens ou de todo alguma. A resolução para este tipo de problemáticas assenta quase sempre numa correcta estruturação do algoritmo que controla o hardware em conjunto com o software [39].

3.3.3 SPOOFING

Um ataque do tipo *spoofing* passa por fornecer ao sistema principal informação falsa, no entanto pretende-se enganar o sistema para que este aceite essa informação. Alguns ataques de *spoofing* envolvem falsificar o nome de domínio, o *Internet Protocol* (IP)

address, ou *Media Access Code* (MAC). Um exemplo de *spoofing* no RFID seria o envio de um EPC falso ao sistema e o sistema aceitar [39].

3.3.4 INSERT OU RFID EXPLOIT

Um ataque do tipo *insert* passa por inserir comandos de sistema em zonas onde dados seriam esperados. Um exemplo típico deste tipo de ataque é o de *SQL injection*, que passa por inserir um comando SQL numa zona de *login* de uma aplicação web, para que dados confidenciais sejam retornados como resposta a este comando SQL. Em RFID este ataque passa por inserir um comando de sistema na zona de interpretação do leitor, aquando da leitura da *tag* que transporta informação [39].

3.3.5 REPLAY

Num ataque do tipo *replay*, um sinal RFID válido é interceptado e os dados são gravados para que possam ser usados mais tarde e transmitidos para o receptor (*play-back*). Os dados serão aceites visto que se encontram válidos [39].

3.3.6 DOS

Ataques DoS são conhecidos por *flood-atacks*. Estes ataques passam por encher o sistema com dados e pedidos, tornando o sistema indisponível devido ao imenso processamento necessário para processar a informação. Uma variante deste ataque chama-se *Radio Frequency Jamming* e passa por introduzir bastante ruído no sinal enviado, tornando-o imperceptível ou impossível de interpretar para o receptor. Estes problemas de segurança pertencem ao nível físico da arquitectura do sistema RFID, os vendedores de *hardware* estão constantemente a inovar para evitar que ataques explicados até aqui ocorram [39].

3.3.7 MIDDLEWARE

Os ataques *middleware* podem ocorrer em qualquer ponto entre o *reader* e a a aplicação (base de dados). O *middleware* localiza-se entre o nível físico e o nível da aplicação da arquitectura. Para eliminar este problema existe *middleware* que implementa soluções de encriptação avançada com o objectivo de proteger esta camada da possibilidade de ataques [39].

3.3.8 BACKEND

Dado que a base de dados é o ponto mais distante do sistema relativamente à *tag* RFID, tanto ao nível dos dados como também a própria distância física entre ambos os elementos, pode-se levar a pensar que a base de dados não é um alvo apetecido pelos atacantes. No entanto se esta base de dados contiver dados como os cartões de crédito dos clientes, relatórios de vendas, este ponto do sistema de RFID passa a ser o mais aliciante para os atacantes. A ligação entre as *tags* e o *backend* passa pelo nível da aplicação, ou seja, os pedidos feitos à base de dados são feitos consoante a actividade das *tags* e a lógica de negócio implementada ao nível da aplicação. Para que seja garantida segurança ao *backend* os programadores que desenvolvem a aplicação de negócio têm que usar ferramentas de segurança disponibilizadas pela infraestrutura que estão a desenvolver de forma a não permitirem acessos maliciosos à BD [39].

3.4 VULNERABILIDADES

Os sistemas informáticos que usam RFID têm características que podem ser vítimas de ataques como por exemplo:

- Linhas de código excessivas - As *tags* de uma forma geral não são problemáticas neste aspecto, mas todo o software que está por trás da identificação pode conter nalguns casos milhões de linhas de código. Estimando que por cada 1 000 linhas de código possam existir entre 6 a 16 *bugs*, as fragilidades são evidentes [35]. Mesmo nas pequenas aplicações podemos encontrar este tipo de dificuldade pois tendo menos linhas de código, sofrem quase sempre de testes insuficientes.

- Protocolos Genéricos - Se se usa a Internet para desenvolver a aplicação sofre-se também das suas vulnerabilidades por uso de ferramentas como DNS, URI e XML [35].

- Bases de Dados - Se pretendemos fazer o controlo de algo temos de o identificar, e para o fazer temos de ter as Bases de Dados armazenadas algures, armazenamento esse que pode ser acedido indevidamente [35]. À medida que esta tecnologia se vulgarizou o interesse dos ataques aumentou em consequência havendo neste momento para os *hackers* todo um mundo de exploração de informação. Alguns dos ataques mais comuns são:

- SQL INJECTION

A base de dados ou a aplicação que manipula os dados da base de dados são alguns dos pontos onde certas vulnerabilidades podem ocorrer. O que as aplicações fazem, tipicamente, é ler as *tags* e registar ou extrair a informação no *backend* que está associada a essa *tag*, no entanto é possível que algumas aplicações usem um método de conversão do ID da *tag* em hexadecimal para ASCII, obtendo assim a informação da *tag* ao invés de obterem apenas um ID. Se os dados recebidos da *tag* não forem tratados correctamente, é possível que esta contenha código SQL que é executado pela aplicação [35].

O exemplo seguinte mostra como isto pode ser feito.

Tabela de Conversão de Hexadecimal para ASCII	
Hexadecimal (Informação na Tag)	**ASCII**
27204f5220507265636f203d202853656c656374204d494 e28507265636f292046726f6d2050726f6475746f 73293b	"' OR Preco = (Select MIN(Preco) From Produtos);"

Tabela 13 Conversão Hexadecimal-ASCII [39]

Comando SQL na aplicação:	"SELECT Preco from Produtos WHERE nome_produto = '@nome';"
Dados em ASCII recebidos da tag:	"' OR Preco = (Select MIN(Preco) From Produtos);"
Resultado:	"SELECT Preco from Produtos WHERE nome_produto = ' ' OR Preco = (Select MIN(Preco) From Produtos);"

Tabela 14 Exemplo de SQL injection [39]

Neste simples exemplo de *SQL injection* o preço retornado (Preco) não é o preço associado ao nome do produto mas sim o preço mínimo (MIN(Preco)) existente na base de dados. Este tipo de problemas pode ser evitado se em vez de ser feita a conversão do hexadecimal para ASCII, for usado directamente o valor hexadecimal da *tag* como referência na base de dados. Outras precauções podem ser tomadas como por exemplo limitar as permissões de acesso à base de dados.

- OVERFLOW DA MEMÓRIA DO READER

Pode não ser intuitivo como é possivel que uma *tag* com o seu tamanho limitado de memória causar um *overflow* no *buffer* do *reader*, mas isto pode acontecer se o *reader* não estiver preparado para receber muita informação [39]. A maioria das *tags* RFID inclui

dados que informam o *reader* previamente quanto ao seu tamanho de memória, quando o *reader* lê esta informação, tipicamente reserva um *buffer* com o tamanho da memória da *tag*. O que pode suceder em certos casos é a *tag* indicar um valor muito inferior de memória comparativamente ao valor que realmente transporta e que irá enviar para o *reader*, o que irá causar um *overflow* do *buffer* [35].

Resumindo, os principais problemas de segurança que podem surgir com esta tecnologia são:

- Violação da integridade física - Uma etiqueta possui dados específicos do material em que está localizada. Se esta for colocada noutro material, pode causar danos ao seu utilizador. Um exemplo: se um ladrão trocar a etiqueta de um produto caro (ex: televisão) com a de um produto barato (ex: pilha), poderá lesar o estabelecimento pois trará prejuízo a este.

- Cópia de etiquetas - Sendo detentora do conhecimento de criação de etiquetas, uma pessoa pode copiar dados de uma etiqueta alheia, usando um leitor, e criar uma nova com os mesmos dados. Se as etiquetas estiverem encriptadas é necessário uma aplicação para desencriptar essa informação. Quanto à clonagem do ID próprio da etiqueta esse só pode ser reproduzido pela recolha de sinais em *hardware*. Um dispositivo electrónico (relativamente simples como o apresentado na figura 28 pode fazer isso).

- Monitorização da etiqueta - Obtenção de dados das etiquetas para uso indevido sem a envolver fisicamente. Exemplo: um ladrão pode descobrir os dados bancários de uma pessoa e, sabendo que esta possui grande quantia de dinheiro, obrigar a que levante o dinheiro num Multibanco.

Um dispositivo como se apresenta (figura 28) pode ser o suficiente para fazer a leitura e reprodução de sinais de etiquetas RFID. Basta aproximar-se, de uma etiqueta e electronicamente ele replica os dados. No caso apresentado, a réplica funciona para etiquetas Verichip, mas para o adaptar a outro tipo de etiquetas basta fazer a conversão da frequência de trabalho do sistema em questão, e do software da aplicação (por causa das possíveis encriptações). Este circuito não faz a reprodução do ID da etiqueta, mas trabalha na mesma gama de operação da detecção de passagem feita pelas lojas de roupa. Para fazer uma reprodução do ID da etiqueta teria de se ter uma leitura muito próxima do objecto, que faz com que a Antena seja alimentada, fornecendo em simultâneo energia à electrónica da

etiqueta que transmite ao leitor o seu ID, que após ter esta informação dá ou não permissão de execução. Neste caso, os sinais baseiam-se na ressonância da antena fazendo a replicação do sinal presencial da etiqueta. Este dispositivo funciona na frequência de 134 kHz, e possui um PIC que através de uma programação e de comparação (sinais), recebe os sinais portadores e faz a sua descodificação. Através da EEPROM, e depois de todas as informações lidas, a informação pode ser emitida para um leitor como se de uma etiqueta se tratasse.

Figura 28 Replicador Tags RFID

Estes são alguns dos problemas que possivelmente trarão mais complicações às pessoas caso a tecnologia RFID seja implementada em larga escala e sem ter o devido cuidado em segurança.

Para colmatar este tipo de questões existem alguns principios básicos que se podem respeitar na concepção:

- SIMPLIFICAÇÃO

Em vez de se utilizarem caracteres especiais, talvez seja mais fácil evitar erros se se usarem os alfanuméricos generalistas (0-9, a-z, A-Z). Nem sempre é possível, mas deve ser referenciável [35].

- LINGUAGENS DE SCRIPT

Tendo algum cuidado em evitar linguagens como Javascript, VBscript e Flash diminuem-se as probabilidades de sucesso no ataque [35].

- BASE DE DADOS

Limitando as possibilidades de acesso às Bases de Dados, alcança-se uma maior margem de sucesso a violações. Estas devem ser disponibilizadas como "Só de Leitura" ou mesmo inacessíveis. Não se devem também permitir as múltiplas execuções de sessões às Bases de Dados [35].

- SERVIDORES

O acesso ao(s) servidor(es) deve estar bem comtemplado. Somente administradores devem poder acedê-lo e de forma alguma se deve facilitar a comunicação com outro tipo de *hardware* do sistema [35].

- REVISÕES

O código base do sistema deve ser sempre visto e revisto de forma não escapar nenhuma vulnerabilidade. Principalmente se for usado em plataformas comerciais [35].

3.5 QUESTÕES ÉTICAS E PRIVACIDADE

As *tags* RFID podem ser usadas para uma série de funções como controlo de armazenamento e identificação de propriedade prevenindo roubo ou perda. Uma loja poderia por exemplo colocar *tags* RFID em todos os seus produtos e os clientes poderiam ter um cartão de crédito que automaticamente debitaria o valor das compras na hora que o cliente saísse da loja, sem precisar passar pela caixa. Mas esse tipo de questões são precisamente as que acarretam problemas.

Se uma loja de roupas decide colocar esses *tags* invisíveis em todas as roupas, o cliente compra e leva para casa. Depois, retorna à loja com a mesma roupa e é reconhecido pelo nome, ou então entra numa loja e recebe sugestões em grandes painéis baseadas em compras passadas.

Mesmo com regulamentação governamental, a situação pode-se tornar rapidamente uma ameaça à privacidade [23]. Principalmente quando os criminosos começarem a aproveitar-se da tecnologia. O mais engraçado é que estudos recentes apontam que as pessoas não estão particularmente preocupadas com a privacidade nesta tecnologia. Este facto deve-se provavelmente ao facto de esta ainda não ter sido amadurecida/divulgada o suficiente para que o público em geral se aperceba dos perigos/ameaças à privacidade que esta pode levantar [23].

A ameaça à privacidade surge quando o RFID permanece activo e o consumidor deixa o estabelecimento. Este é o cenário que deve alarmar as pessoas e neste momento a indústria de RFID parece dar sinais mistos sobre se as *tags* devem ser desactivadas ou deixadas em activo por padrão.

Uma das possibilidades seria a de deixar o cliente escolher se quer manter as suas *tags* activas ou não, e informar o estabelecimento caso este opte por desactivá-las [23].

Para respeitar a privacidade dos consumidores, os estabelecimentos devem seguir 4 premissas essenciais:

- Os consumidores devem ser notificados quanto à presença de RFID nos produtos, e em quais deles isto acontece;
- As *tags* RFID devem ser desactivadas na saída da caixa do estabelecimento;
- As *tags* devem ser colocadas na embalagem do produto, e não nele próprio;
- As *tags* RFID devem ser bem visíveis e facilmente removíveis.

3.6 DESAFIOS ACTUAIS

Embora nos últimos anos tenham havido avanços consideráveis na tecnologia RFID, diversos desafios ainda são reais para uma ampla expansão.

Estes desafios concentram-se muito na aplicação que é feita do dispositivo, sendo que para determinados usos a tecnologia está razoavelmente consolidada, enquanto que para outros ainda deve ser desenvolvida. Os que se sobressaem são:

- Preço - embora actualmente os preços destes dispositivos estejam competitivos a ponto de substituir inclusive códigos de barra em produtos, para produtos de baixo valor (e baixo lucro) esta substituição não se mostra vantajosa, por isso a tendência é estar a ser feita primeiro em produtos de alta margem de lucro;

- Poder de processamento e fornecimento de energia - Para dispositivos com RFID activo, o tempo de vida da bateria ainda é um problema generalizado entre os dispositivos móveis, sejam computacionais ou não. A curta duração da carga das baterias actuais limita o desenvolvimento de novos dispositivos e aplicações, pois estes requerem mais poder de processamento, que por sua vez requer maior fornecimento de energia. Para dispositivos com RFID passivo, embora eles sejam alimentados no momento da utilização pelo leitor, a carga obtida por esta alimentação é proporcional à distância a que este se encontra do leitor, de modo que quanto mais distante menor a carga obtida. Isto também limita o desenvolvimento de novas aplicações, obrigando-as a ficarem mais próximas do leitor para receberem a carga apropriada para o processamento, o que pode fugir completamente do propósito da aplicação;

- Distância de leitura - Independentemente do problema do poder de processamento, algumas aplicações podem requerer que a identificação de dispositivos com RFID seja feita a muitos metros de distância, o que ainda não é suportado;

- Miniaturização: embora pequenos o suficiente para serem colocados em etiquetas, algumas aplicações podem necessitar de dispositivos RFID imperceptíveis à visão e ao tacto, para permitir a sua total integração à rotina das pessoas.

3.7 COMPARAÇÃO TECNOLÓGICA

Na tabela 15 são demonstrados alguns factos de comparação entre alguns dos sinais mais utilizados na actualidade. Ressalta a grande velocidade e a enorme funcionalidade do RFID face aos restantes apresentados. Vem um pouco também na sequência do surgimento histórico e da consequente evolução dos mesmos.

	RFID	IrDa	Bluetooth
Tempo de Operação	< 0.1 ms	~0.5 s	~6 s
Alcance	De 3 a 10 m (Comum)	Até 5 m	Até 30 m
Uso	Variadíssimos Dispositivos	Somente alguns dispositivos e para pequenas trocas	Dispositivos de Dados
Selectividade	Proximidade	Linha de Vista	Identificação e confirmação
Aplicações	P.Ex. localização de itens	Controlo e Troca de dados	Rede para troca de dados e para auriculares
Experiência consumidor	Obtenção Informação	Fácil	Configuração Obrigatória

Tabela 15 Comparação Sinais "wireless" [40]

3.8 FUTURO DO RFID

A tecnologia envolvida num sistema RFID promete inovar a forma como são geridos os negócios, aumentar lucros e reduzir custos operacionais. A questão coloca-se em como traduzir o RFID numa vantagem competitiva organizacional. O valor estratégico centra-se, actualmente, nas seguintes áreas chave:

• Gestão de cadeias de fornecimento;

• Gestão de bens e produtos;

• Segurança e controlo de acessos;

• Aplicações para os consumidores;

• Processos da indústria transformadora.

Foi previsto que no ano de 2010 a tecnologia de RFID tenha investimentos de mais de 2 milhares de milhão de euros por ano a nível mundial. A tecnologia de RFID será impulsionada pelo facto de que em algumas aplicações era impossibilitado o uso de código de barras e a distribuição em larga escala pelos sectores emergentes será evidente.

O RFID não deve ser um substituto dos códigos de barras. As duas tecnologias vão coexistir, aplicando-se uma ou outra à situação mais conveniente.

A tecnologia será aplicada pelas empresas conforme a necessidade de cada uma, as de logística e de farmácia por exemplo tendem a adoptar mais rapidamente que as demais. Isso deve-se à necessidade de combater a falsificação de produtos.

Estão neste momento em teste algumas soluções que se poderão vir a revelar como decisivas no futuro da tecnologia.

3.8.1 NOVAS SOLUÇÕES/TECNOLOGIAS

Estão já em desenvolvimento tecnologias que permitem descobrir *tags* em qualquer faixa de frequência, o que na prática se traduz numa maior facilidade de leitura e autenticação de uma *tag* mesmo quando esta se move rapidamente – até uma velocidade de 240 km/h. Este protocolo oferecerá benefícios ao nível do transporte e logística, gestão de cadeia de fornecimento e outros processos. Além disso, a utilização destas *tags* de baixa frequência poderá ser utilizada para rastrear matérias perigosas tanto ao nível da palete, como da caixa ou até mesmo da unidade. Também do ponto de vista do cliente a implementação destes sistemas será vantajosa, pois permite-lhes obter as *tags* – fornecidas num autocolante – sem qualquer custo adicional. Em termos de alcance este sistema conseguirá ler as *tags* até uma distância máxima ligeiramente superior aos 5 metros [39].

3.8.1.1 TAGS PARA MATERIAIS DIELÉCTRICOS

A presença de metal ou de outros materiais dieléctricos – como a água – são, ainda, um dos grandes obstáculos à utilização da tecnologia. Estes materiais desviam as frequências de ressonância de tal forma, que estas deixam de receber a potência emitida pelo *reader*. Estas etiquetas que têm isoladores sincronizam a frequência da *tag*, permitindo assim que possam ser aplicados neste tipo de materiais. Existem por isso isoladores UHF específicos para cada *tag* [39].

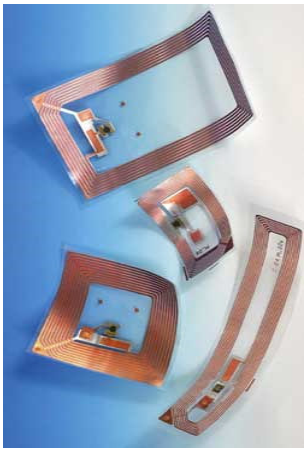


Figura 29 Tags com materiais isoladores

3.8.1.2 TAGS RESISTENTES A TEMPERATURAS ELEVADAS

Uma empresa suíça, criou *tags* específicas para suportar as altas temperaturas características dos processos de produção alimentar, podendo, no entanto, ser utilizada também em ambientes industriais ou em exteriores. Esta *tag* é disponibilizada tanto em baixa como em alta-frequência, e é indicada para identificar aqueles itens que são regularmente sujeitos a altas temperaturas ou situações de *stress* mecânico, onde se incluem objectos sujeitos a limpeza em água quente. As *tags* encontram-se sob as normas da UE de modo a que possam ser usadas directamente em contacto com comida ou bebida. Conseguem aguentar temperaturas até aos 140ºC durante muitas horas, usando um invólucro de uma nova geração de plástico térmico [39].

Figura 30 Tags alta temperatura

3.8.1.3 TAGS GLOBAL LOOP

Esta *tag* possui um desenho inovador que pode ser usado com frequências da América do Norte, Europa ou Japão. É uma EPC de segunda geração e que foi pensada especificamente para ser colocada em materiais que bloqueiam as ondas RF das actuais tags RFID, ou seja, materiais altamente refractores ou reflectores de ondas electromagnéticas, como por exemplo a água, ou então objectos ou mesmo outros equipamentos electrónicos que possam gerar interferências. O novo desenho permite também elevados níveis de fiabilidade quando a orientação do produto não é fixa ou pode ser alterada após aplicação da *tag*. Tem dimensões na ordem dos 7 cm de lado e pode ser usada nas frequências de 860 a 960 MHz com mínima degradação de performance. Uma *tag* com estas características

permite que o seu uso seja expandido a muito mais ambientes, evitando a escolha de *tags* específicas para determinado tipo ou natureza de produto [39].

3.8.1.4 TAGS RUBEE

RuBee, também conhecido como P1902.1, é antes de mais um protocolo desenvolvido, para representar *tags*, tanto activas como passivas, que operam a uma baixa frequência, 132 kHz, e cujo objectivo é serem capazes de catalogar, com elevada eficiência, produtos compostos por materiais que interfiram com a tecnologia RFID. A maioria das *tags* HF e UHF usam, principalmente, a porção rádio da indução electromagnética para transmitir o seu sinal. Estas *tags*, porém, usam 99.9% de ondas magnéticas e 0.1% de ondas rádio, uma vez que as ondas magnéticas não são atenuadas pela água. As baixas frequências são também menos afectadas pelo metal. Alguns produtores de *tags* UHF passivas estão a começar a desenhar *tags* optimizadas para reflectir sinais usando o campo magnético, para quando está nas proximidades de um *reader* e usar os sinais rádio (que conferem um maior alcance com frequências mais elevadas), quando o *reader* está mais longe. Isto permite também uma melhor distinção entre produtos a curto-alcance, como por exemplo num carrinho de compras num supermercado [39].

3.8.1.5 TAGS DESTACÁVEIS

Um problema que é imposto por toda a questão das *tags* inseridas nos produtos, até ao nível do consumidor, é a questão da privacidade. Uma desactivação ineficaz, ou não existência de desactivação das *tags* dos produtos adquiridos pelos consumidores finais, implica que qualquer detentor de um *reader* conseguirá obter a informação dos produtos adquiridos por dada pessoa, o que constitui, obviamente, uma quebra na privacidade individual [39].

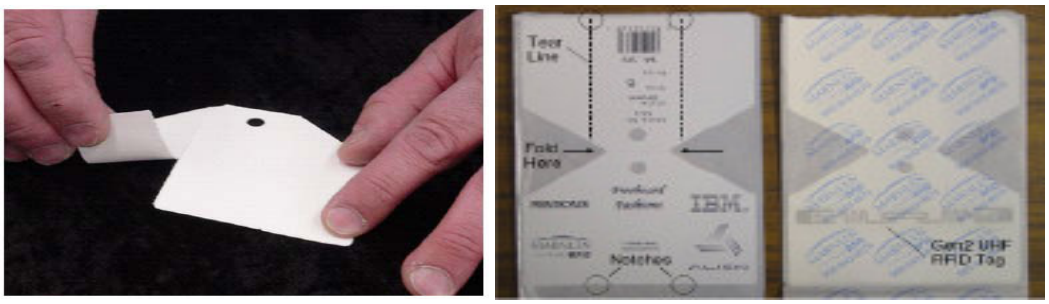


Figura 31 Forma e utilização da Tag destacável [39]

Pensando nisto, a IBM criou a sua própria *tag* destacável, dando ao utilizador a possibilidade de literalmente rasgar a *tag* pelo picotado, "arrancando" as antenas da *tag*, cortando assim o seu modo de comunicação, ou então arrancando o próprio *chip*. Quanto aos leitores podem ser usadas com qualquer um que esteja baseado na leitura de etiquetas Geração 2 em UHF.

3.8.1.6 STRONGHOLD TAGS

Com o lançamento dos novos passaportes e cartões RFID, lança-se também a preocupação em relação à invasão de dados pessoais e/ou confidenciais guardados em tais suportes, tais como números de cartões de crédito, identificação pessoal e até palavras-passe. Assim sendo, criou-se o "bloqueador de intrusos" em forma de saco para passaportes que pode ser, por exemplo, facilmente cozido ao interior de um casaco ou a outras peças de roupa. Ainda que este saco seja desenhado para esse efeito, ele conseguirá de facto bloquear praticamente todos os sinais de rádio, inclusive sinais de telemóvel. Este saco é tecido em camadas de níquel, cobre e prata, bloqueando as ondas de rádio no seu interior, devido a esta liga altamente absorvente para sinais rádio [39].

Figura 32 Saco Anti-RFID e pormenor do tecido [39]

3.8.1.7 IMPRESSORA TAGS

Esta tecnologia usa um tinteiro que possui fluido de prata no seu interior e que, em conjunto com a impressora, consegue imprimir, com alta precisão, gotas na ordem do picolitro (1.0×10^{-12} litro) de materiais orgânicos ou inorgânicos, numa grande variedade de substratos [39].

Figura 33 Impressora Tags [27]

Com tal tecnologia, é possível imprimir materiais com camadas múltiplas de gel, metal, polímero condutor ou material orgânico e emissor de luz. Apesar de possuir muitos outros usos possíveis, torna-se possível imprimir o circuito de uma *tag* numa variada gama de substratos. A impressão das informações das etiquetas (papel) é feita como numa vulgar impressora e simultaneamente escreve-se a informação digital no *chip* embebido. Ao mesmo tempo que processa a impressão pode ler, gravar e imprimir etiquetas e rotulos com *transponders* RFID embutidos que são programados e re-programados usando ondas de rádio - RF.

3.8.1.8 MOBILE RFID

Este tipo de tecnologia é ainda bastante recente mas pode-se assumir como líder no mercado emergente. Trata-se da utilização do equipamento mais pessoal e portátil do nosso quotidiano – o telemóvel – como meio para a identificação por rádiofrequencia. Dotando este dispositivo de um leitor/emissor RFID facilmente se conseguem fazer leituras (e até escritas) em *tags*. Depois a partir de *software* esse sinal pode ser descodificado para corresponder por exemplo a uma base de dados ou a uma qualquer informação que possa ser útil para a execução de um determinado serviço ou identificação de produto. O passo seguinte resume-se a tratar essa informação e enviá-la através de uma rede comunicacional por um qualquer protocolo como por exemplo WAP ou Wi-Fi [16]. A recepção deste sinal é feita por uma *Gateway* do receptor que a descodifica por ONS respeitante aos protocolos EPC de acesso (figura 34).

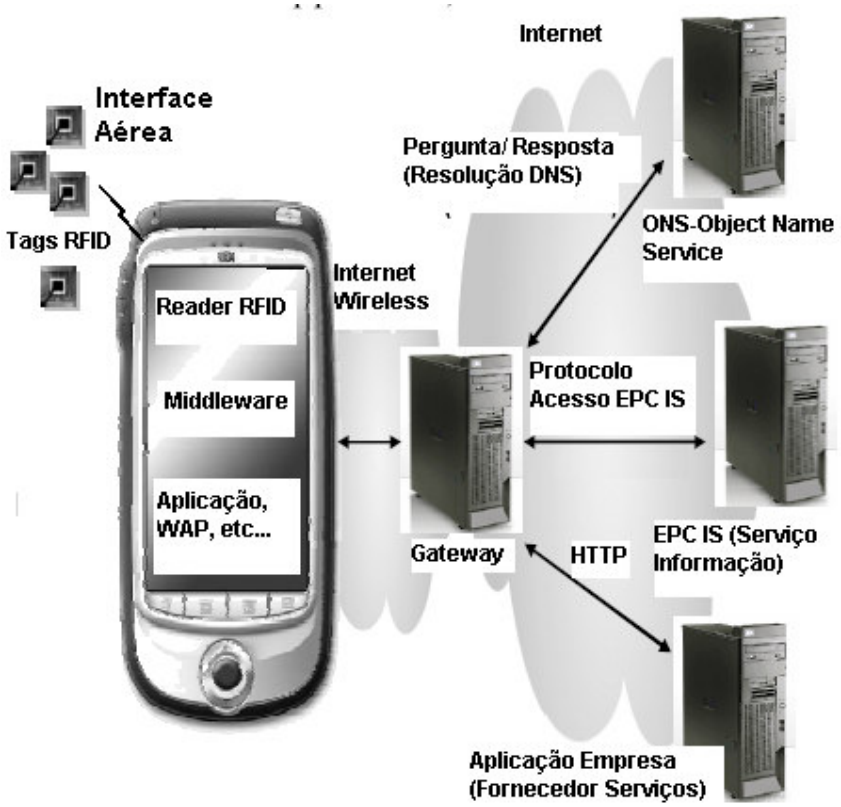


Figura 34 Arquitectura Sistema Mobile RFID

No caso de querermos fazer reencaminhamentos depois do sinal transmitido há toda uma possibilidade de execução pelas várias normas conhecidas como *http* ou outras. Podem-se por exemplo identificar/comprar produtos que possuam *tags* e fazer reservas sem termos de recorrer ao comum cartão de crédito. Comprar um bilhete pode vir a ser tão fácil como encostar o telemóvel a um poster publicitário do evento (figura 35). Não existem limitações por isso de mobilidade e os dados de várias escritas/leituras podem inclusive ficar armazenadas no dispositivo. Há ainda a vantagem/desvantagem de localização em tempo real do utilizador do serviço através das redes GSM e 3G [34].

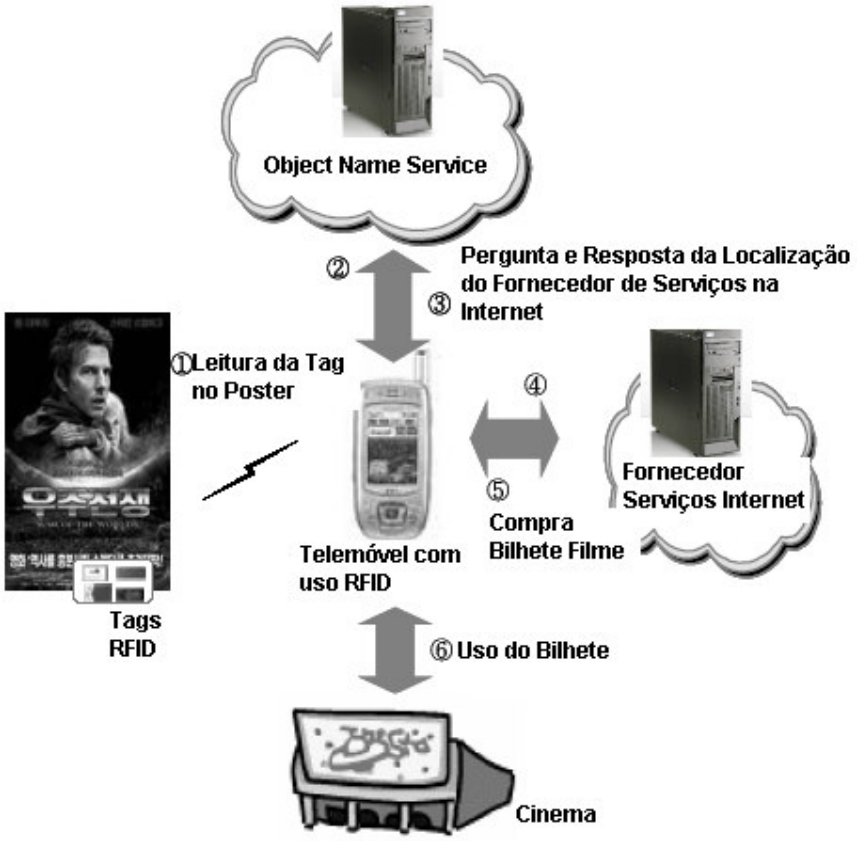


Figura 35 Compra Bilhete por RFID [39]

No Japão os telemóveis que trazem incorporado a tecnologia RFID têm tido um grande sucesso, a utilização destes terminais é feita nas viagens de comboios. Para facilitar a viagem de comboio, a Mitsubishi desenvolveu um aplicativo que permite aos utentes deste serviço saberem exactamente onde se encontram, qual o percurso, ligações e paragens devem percorrer para atingirem o seu destino. Os utilizadores deste serviço têm apenas que encostar o telemóvel a alguns *hotspots* localizados em vários pontos das carruagens, para que possam receber esta informação [39].

Figura 36 RFID nas carruagens de comboios [39]

3.9 POSSÍVEIS PROBLEMAS FUTUROS

Alem dos citados no sub-capitulo da Segurança, foi criado recentemente o primeiro vírus capaz de se auto-replicar por meio de etiquetas RFID. Se alguns tipos de vulnerabilidades estiverem presentes no software de RFID, a etiqueta infectada (intencionalmente) poderá transmitir o vírus para a base de dados utilizado pelo programa que por sua vez, transmite esse vírus para outras etiquetas RFID.

3.10 CONTRAMEDIDAS

No meio de tantas possibilidades de violação da segurança, existem estudos para que a tecnologia RFID seja implementada sem causar danos aos seus utilizadores.

Algumas soluções que estão em teste são:

- CRIPTOGRAFIA

Assim como é utilizado nas mensagens electrónicas (*e-mails*), a tecnologia faz com que somente emissor e receptor possam ter acesso a informação contida na etiqueta. Qualquer pessoa que tente obter esses dados ilicitamente terá que decifrar um código já comprovado como altamente confiável.

- CÓDIGOS

Neste caso, o conteúdo da etiqueta só poderia ser usado mediante o uso de um código. Por exemplo: num supermercado, o utilizador deveria usar um código para validar a compra usando RFID

- DISPOSITIVOS METÁLICOS

Envolvida com estojo feito de um material reflexivo (estudo indica o alumínio como principal candidato), a etiqueta ficaria livre de intercepções quando não estivesse em uso.

- MATAR OU ADORMECER UMA TAG

Existem já endereçamentos de *tags* EPC que doseiam a privacidade dos dados. Quando uma destas *tags* recebe um comando *kill* de um leitor – habitualmente quando são comprados os objectos a controlar – esta desactiva-se a si própria permanentemente [32]. À primeira vista, matar uma *tag* parece ser uma solução de protecção de privacidade muito eficaz, mas elimina todos os privilégios de pós-venda ao utilizador, pois todo o serviço de devoluções, reparações ou aplicações não funcionarão com *tags* desactivadas. Alem disso no caso de librarias e de lojas de aluguer de produtos, as *tags* não podem ser mortas pois têm de sobreviver ao longo do tempo de vida útil do objecto a que estão anexadas. Por este motivo esta solução deve ser ponderada somente para serviços que impliquem de facto soluções de privacidade restrita do utilizador. Ao invés de a matar pode-se somente adormece-la, o que se revela vantajoso pois pode-se de seguida acordá-la. No entanto temos de ter em atenção a questão de que se um leitor a pode acordar, então uma manipulação do sinal desse mesmo leitor pode executar a mesma função com todas as desvantagens inerentes [34].

- TAG COM PASSWORD

As *tags* actuais possuem recursos suficientes para verificar PIN ou *passwords*. Uma *tag* pode emitir informação importante somente se receber por exemplo uma determinada palavra-chave. O paradoxo nesta solução encontra-se na razão de que o leitor não pode conhecer essa palavra-chave, de forma a transmiti-la à *tag* a não ser que conheça a identidade da *tag* [34].

- ENCRIPTAÇÃO

Encriptar o identificador de uma *tag* pode ser uma boa solução para resolver questões de privacidade, mas não os resolve todos, porque a encriptação do identificador é por si só uma nova identificação. Em adição a este problema, existe a questão da manipulação das chaves no esquema de encriptação. Ainda pior do que isso é a pertinência do custo associado. Existem uma série de investigações neste domínio para optimização, mas será complicado avançar com uma solução definitiva a curto prazo devido precisamente aos custos [34].

- EQUIVALÊNCIA A UM PROXY

Em vez de se confiar em leitores de RFID públicos para garantir protecção de privacidade, os utilizadores podem criar os seus próprios meios de o fazer como por exemplo através de dispositivos móveis. Têm sido feitas diversas investigações na perspectiva de se utilizarem soluções na perspectiva de um endereço ou domínio *Proxy* como por exemplo através de temporizadores *Watchdog* embutidos em *tags* [34].

- BLOQUEIO

A *tag* de bloqueio tem sido também objecto de discussão porque previne a utilização não autorizada. Não envolve modificações nas *tags*, mas sim de uma incorporação nas mesmas de um bit modificável denominado de "bit de privacidade". Um "0" no bit de privacidade identifica a *tag* como de acesso público, e um "1" demarca-a como privada [34].

3.11 PROTECÇÃO

- LEGISLAÇÃO

Uma das recentes propostas mundiais feitas pelos CASPIAN – Organização de Cidadãos Americanos com direitos nos RFID – pode ser interpretada como a primeira do género a ser feita de forma legal para proteger os direitos de privacidade dos utilizadores. Esta proposta reclama sobre todas as aplicações RFID por identificação de número de série obrigatório em todos os produtos e privacidade absoluta dos dados de utilizador em aplicações de índole pessoal. Também a EPCglobal publicou uma série de linhas mestras para a definição destes parâmetros da privacidade. Reclamam acima de tudo o aviso aos

utilizadores de algumas características dos sistemas e educação do consumidor para a tecnologia presente. Fala-se muito acerca das licenças que podem/devem ser atribuídas a este tipo de equipamentos, precisamente na perspectiva da protecção do utilizador, com o seu consentimento, claro [34]. A ideia seria ter uma plataforma/organização que detivesse os dados de licenças fornecidas/consentidas por utilizadores e o software fazia uma ligação para atestar a respectiva autorização ou não do controlo de acesso – seria provavelmente a solução ideal [24].

3.12 SOLUÇÕES

- Num futuro próximo, poderá surgir algo semelhante relativamente a tentar-se colmatar a pirataria de DVD, CD, Blu-ray, HD DVD e outros tipos de suporte. O objectivo poderá ser atingido colocando *readers* nos leitores, de modo a que quando o utilizador insira um disco no leitor, o *reader* verifique se o disco é ou não uma cópia e até se está ou não a ser usado na região geográfica devida. Tudo isto permitirá proteger os interesses e a propriedade das companhias de música, estúdios cinematográficos e empresas de jogos e software em todo o mundo. Todo o processamento de comparação de *chips* e leitura dos mesmos será feito em *hardware*, evitando o uso de controladores ou *software*, de modo a que não se possa circundar esse mesmo mecanismo.

- Foi criado recentemente um cartão (figura 37) que usa tecnologia RFID para transmitir a sua informação em longo alcance, mas que apenas opera quando é desligada a "barreira biométrica", isto é, quando o dono do cartão coloca o seu polegar no *scanner* de impressão digital integrado no cartão, de seu nome *IronGate biocard*.

Figura 37 IronGate biocard

Esta solução é por isso apropriada para aplicações na área da segurança pessoal, controlo de acesso de veículos e instalações industriais. A informação biométrica encontra-se armazenada no interior do próprio cartão, por medida de segurança, e uma vez registada a impressão digital de um utilizador num cartão, mais ninguém poderá aceder aos seus dados ou usar aquele cartão. Se no acto do registo do cartão, este se encontrar numa área coberta pelas antenas do sistema, a autenticação automática será efectuada com este, através de um certificado digital, sendo que toda a informação transmitida é encriptada com um algoritmo patenteado. Funciona também com um leitor de cartões, como aqueles que vemos à entrada do nosso banco. Dependendo do tipo de técnica usada (RFID activo ou passivo) o alcance destes cartões vai de cerca de 7 m a 100 m. O *IronGate* é assim um forte candidato a modelo para a próxima geração de cartões de crédito.

4. ÁREAS DE APLICAÇÃO

O objectivo desta secção é apresentar algumas das ideias, conceitos e apostas que têm vindo a surgir fruto do enorme potencial que o RFID apresenta neste momento. Actualmente verifica-se no mercado uma grande necessidade de optimização de lucros e de esclarecimento de posicionamento no mercado do RFID, isto porque a possibilidade deste negócio aumentar em dez vezes o seu volume de negócios nos próximos dez anos constitui enorme atractivo e ninguém pretende ficar de fora.

Existem actualmente imensas ideias e conceitos sobre em que aplicar o RFID. Estudos de mercado continuam a indicar que o RFID passivo continua a ser a escolha prevalecente (com 28%), no entanto os indicadores apontam para um aumento de utilização de *tags* RFID.

Aproximadamente 29% do mercado de utilizadores de RFID utiliza *tags* activas e, 40% dos inquiridos referiu que pensa vir a utilizar esta tecnologia.

Quanto ao tipo de aplicações as áreas em que se esperam haver mais progressos são o controlo de bens e aplicações de logística. Actualmente, no entanto, o controlo de acessos e identificação pessoal são as aplicações mais utilizadas no mercado (aproximadamente 28%). O controlo de bens, gestão de cadeias de fornecimento e controlo de inventário irão

crescer cerca de 60% [28]. Existe ainda outros tipos de aplicações das quais são esperados crescimentos moderados:

• Controlo de acesso de veículos;

• Identificação de documentos e controlo;

• Rastreio de animais;

• Rastreio de produtos farmacêuticos;

• Rastreio de pacientes e equipamento numa unidade de saúde;

• Medidas anti-contrafacção;

• Segurança alimentar.

4.1 SAÚDE E INDÚSTRIA FARMACÊUTICA

Nesta área há já uma diversificação de utilizações das quais se destacam:

- Implantes Humanos - Um pequeno *chip* RFID debaixo da pele, poderá transmitir um número e automaticamente aceder a um completo registo de saúde. Funcionários de hospital, remédios e equipamentos também podem ser etiquetados, criando um potencial de administração automática, reduzindo erros e aumentando a segurança. São etiquetas injectadas no tecido do braço que usando um leitor, os médicos e a equipa de funcionários do hospital podem procurar a informação das microplacas, tais como a identidade do paciente, o seu tipo do sangue e os detalhes da sua condição, a fim de apressar o tratamento [39].

- Cirurgias - Existem kits próprios, específicos para um tipo de operação, que possuem instrumentos que não podem ser etiquetados, e que previamente têm de ser esterilizados. As tags podem estar incluídas transmitindo informação da última esterilização ou de que *kit* faz parte determinado instrumento médico. E quem refere estes equipamentos deve também referir os de maiores dimensões e consequentemente mais caros como por exemplo ventiladores, aparelhos de electrocardiogramas, bombas de infusão, etc. Isto significa que o pessoal do hospital pode encontrar material fora de sítio muito rapidamente aumentando em

consequência a eficiência. Estima-se que se podem obter ganhos mensais na casa dos 8 000 minutos, para não referenciar o facto de que pode salvar vidas em situações particulares [26].

- Lentes especiais - Com um *transponder* implementado no olho de um paciente com glaucoma. O glaucoma é uma doença a qual gera o aumento da pressão interna do olho e que vai tornando o campo de visão cada vez mais estreito; mas as medições de pressão não podem ser feitas a não ser através da cirurgia, portanto, o uso de uma micro *tag* com um medidor de pressão implementada no olho do paciente como numa cirurgia de cataratas, pode comunicar-se com um leitor fora, fazendo assim medições exactas, salvando visões.

- Indústria farmacêutica - Está a adoptar as etiquetas inteligentes para combater a falsificação de medicamentos. Preve-se a identificação, com *tags* electrónicas, de todos os frascos dos medicamentos. A ideia é oferecer às farmácias e distribuidores uma espécie de selo de garantia da autenticidade do produto com o código electrónico, que é único, gravado no *chip* da etiqueta [37].

4.2 CONTROLO DE ACESSOS, BENS E PRODUTOS

4.2.1 TRANSPORTES

- Por exemplo, RFID fixados nos pára-brisas de carros alugados podem armazenar a identificação do veículo, de tal forma que as companhias possam obter relatórios automaticamente usando leitores de RFID nos estacionamentos, além de ajudar na localização dos carros (portal na figura 38) [9].

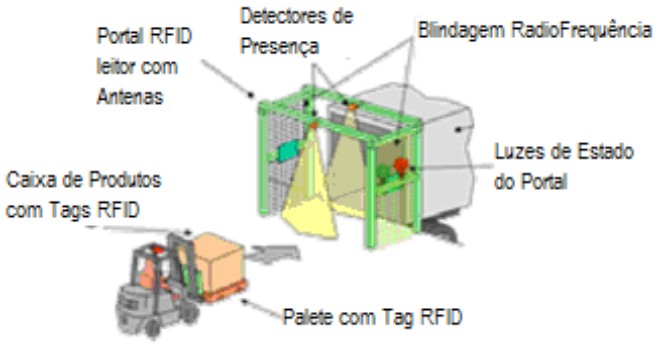


Figura 38 Aplicação em Portal de Passagem (Transportes)

- As empresas aéreas também podem explorar os leitores. Colocando RFID nas bagagens, pode-se diminuir consideravelmente o número de bagagens perdidas, pois os leitores identificariam o destino das bagagens e direccionariam de forma mais eficiente. O **aeroporto de Los Angeles** procurou no RFID uma forma de reduzir as perdas e atrasos na recepção de bagagens [38] (exemplo figura 39).

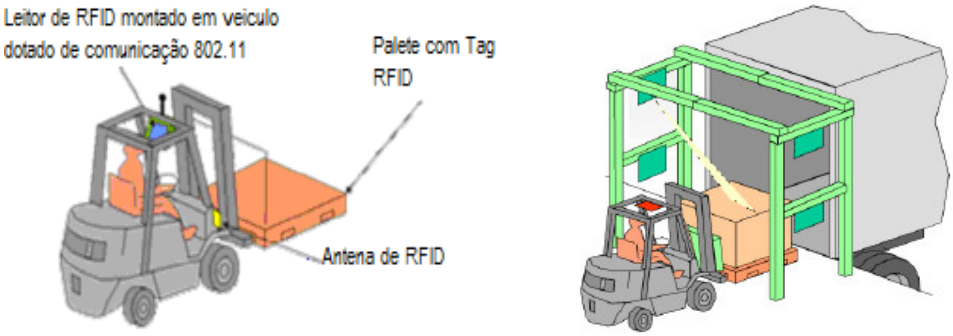


Figura 39 Aplicação em veículo e objecto

- A **Metro do Porto** sustenta numa solução RFID o novo sistema de bilhética sem contacto que controla os acessos à rede de transporte urbano. A identificação do cliente passou a estar contida no suporte RFID, dispensando a utilização mensal de papéis na emissão de bilhetes e passes. Ao mesmo tempo, foi possível diminuir os índices de fraude e melhorar a qualidade do serviço prestado ao cliente, que perde menos tempo no acesso ao transporte [30]. Esta solução é usada similarmente um pouco por toda a Europa com a tecnologia Philips Mifare que detem um bom rácio de dados formatados assim como dispositivos de segurança [29].

- A empresa global de logística, Schenker, iniciou uma fase de testes, com a tecnologia RFID, para rastrear contentores (figura 40) utilizados para envios de longa distância. O contentor chega, é registado no sistema através de RFID, quando sai das instalações para ser entregue passa de novo por um portal RFID. Quando chega ao cliente final este regista-o de imediato tambem por este método. As bases de dados de fornecedor e cliente devem ser partilhadas, sendo que desta forma todas as partes tem acesso ao percurso do contentor/produto com pormenores. Este teste iniciou-se na sua subsidiária alemã, Deutsche Bahn, que colocou tecnologia RFID em 10 dos seus contentores. Estima-se que por exemplo se um ponto de venda ficar sem armazenamento de um produto, com RFID consegue fazer a

reposição até 3 vezes mais rápido do que com processos habituais. Os roubos de mercadorias existentes por exemplo em armazéns reduzem-se em larga escala pois o acompanhamento mais uma vez é feito *in loco*. Todas estas características se revelam importantes na qualidade/preço final do produto e na impressão tida pelo cliente que tem ganhos também nestes pontos e na pós-venda [39].

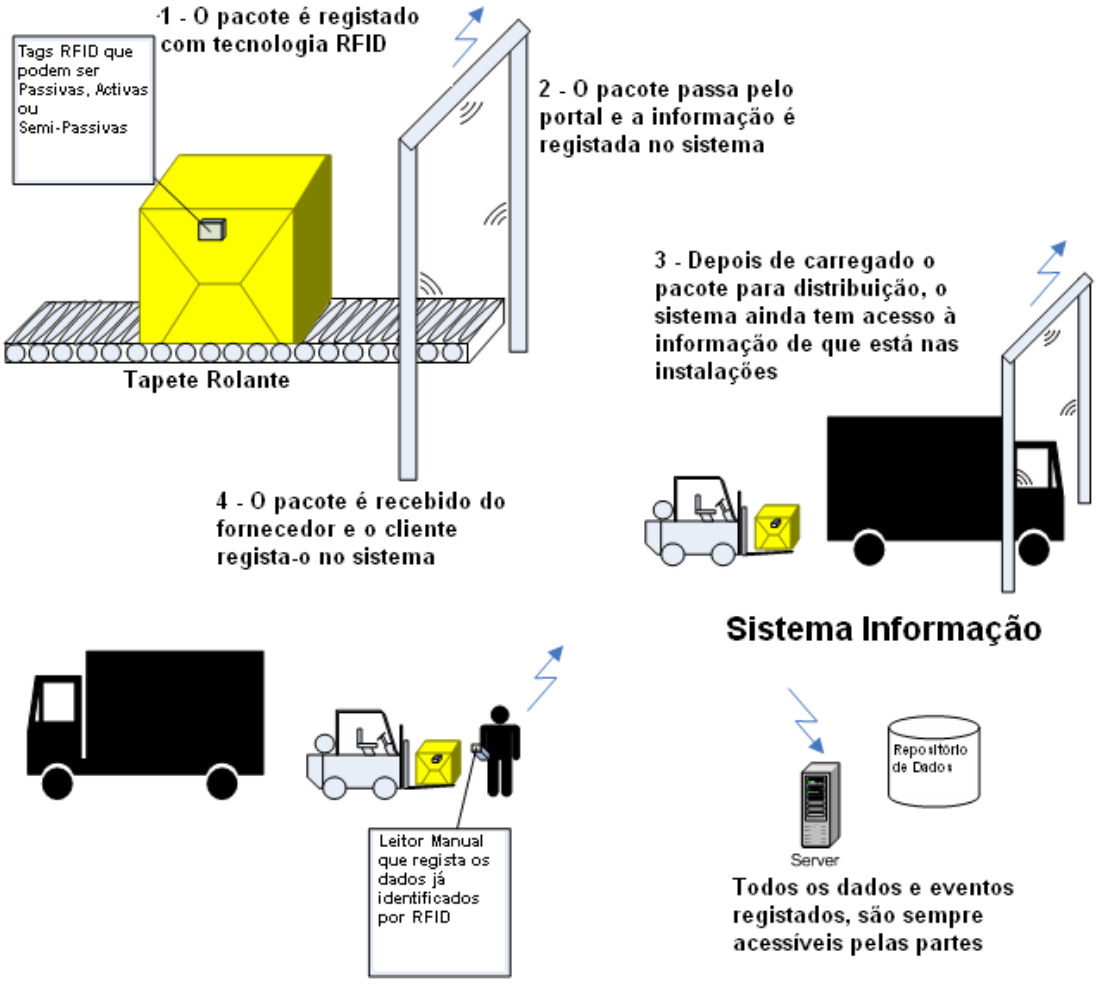


Figura 40 Modelo de um Sistema RFID em logística [33]

Esta solução permitirá que os contentores sejam automaticamente registados onde a responsabilidade pelos bens mude, no entanto há mesmo assim que ter em atenção por exemplo os dimensionamentos porque no caso específico do tapete rolante os objectos podem estar a passar a uma velocidade considerável a distancias que não são superiores a 10 cm nalguns casos, requisitando do *reader* maior potência consumida para que todos os objectos possam ser lidos. Este é um caso flagrante

em que não pode haver dificuldades de leitura em velocidade, ou latências [29]. Desta forma essa encomenda ficará imediatamente visível em pontos fulcrais da cadeia de distribuição [38].

- Os Correios de Espanha implementaram um sistema de identificação/localização por radiofrequência para acompanhar o percurso dos seus envelopes no sistema postal. O organismo, que adoptou este serviço de identificação por radiofrequência em 10 000 cartas-piloto por mês, pretende detectar problemas nos envios e melhorar o serviço. Foi investido 1 milhão de euros neste projecto, e a longo prazo a tecnologia será ainda mais avançada e estendida a todo o serviço de correios. Os correios já adquiriram 5 000 etiquetas electrónicas, 1 900 antenas fixas e 330 leitores. A implementação total do serviço irá permitir um controlo absoluto do sistema postal espanhol, estando a organização bastante segura das funcionalidades e do serviço. A empresa explica que os 10 000 envios mensais do projecto-piloto são realizados através de entidades externas, o que significa que, por agora, não se utiliza RFID nos envios regulares. As etiquetas utilizadas pelos correios são etiquetas passivas, isto é, só emitem a informação quando em contacto com uma antena, sendo assim inócuas. Para além disso, este organismo gere 5 000 milhões de envios postais por ano e chega diariamente a mais de 19 milhões de domicílios. No entanto, o seu uso generalizado seria um investimento demasiado avultado, por essa razão os correios querem implementar somente em envios de estafeta. Cada vez que uma carta com etiqueta passa por uma antena o leitor envia os dados com data e hora do envio, bem como a respectiva matricula [39].

4.2.2 INDÚSTRIA

Hoje em dia, a maioria dos sistemas que gerem os recipientes é baseada em códigos de barras, porém no meio industrial o uso deste tipo de sistema não é confiável o suficiente, e os *transponders* de um sistema RFID podem guardar mais informações úteis posteriormente, como o dono do recipiente, conteúdo, volume, preenchimento ou pressão máximos e dados de análise, além dos dados poderem ser mudados e um mecanismo de segurança poder ser implementado, evitando escrita ou leitura não autorizadas (exemplo figura 41) [9].

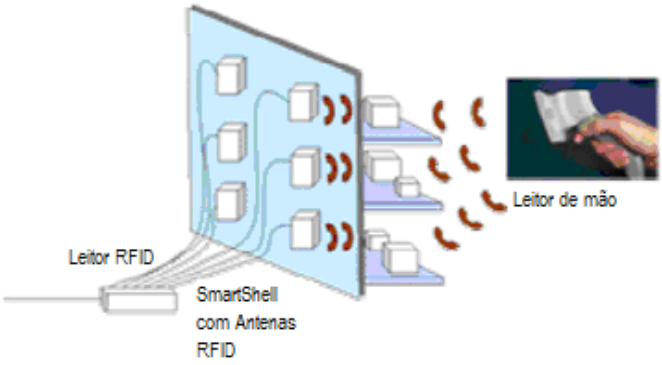


Figura 41 Montagem em prateleiras

As *tags* usadas são de acoplamento indutivo, trabalham numa faixa de frequência < 135 kHz e têm que aceitar condições hostis, como poeira, impactos, radiação, ácidos e temperaturas muito altas ou muito baixas (de -40ºC a +120ºC) (figura 42).

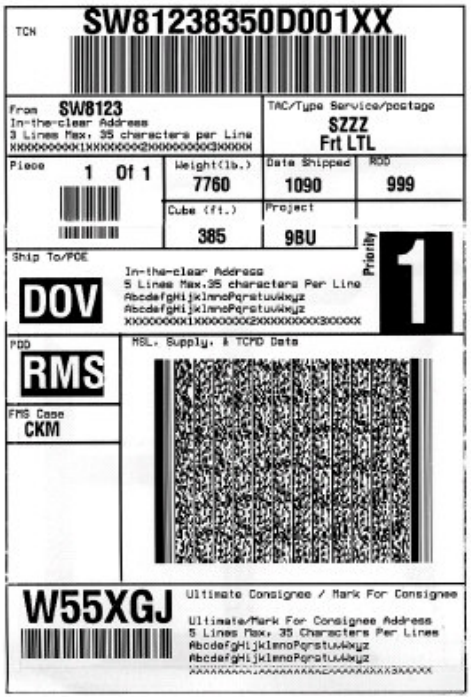


Figura 42 Etiqueta presente nas embalagens [27]

Têm vasta utilização para áreas diversificadas que envolvam este tipo de condições de operação. São etiquetas constituídas por um *chip* de pequeníssimas dimensões com espessuras equivalentes à de uma folha de papel, envolvido por uma camada de pistas que servirão de antena e de meio de comunicação com o chip e o leitor. Um dos métodos de

fabrico consiste em deter um filme laminado de folha metálica que irá ser soldado a um elemento base da superficie. Este filme laminado é o que segundo um determinado padrão irá constituir a antena. De seguida faz-se a soldadura juntamente com um material protector deste filme metálico aos portos do chip que contem as informações da etiqueta. Existem duas camadas essenciais de constituição e entre estas camadas é onde existem todos os fenómenos de condução de calor, pressão e de extracção de humidades com o uso de rolos de desidratação e de secagem para a "assemblagem" da etiqueta.

Quanto ao sector industrial em específico, os sistemas de RFID têm várias aplicações.

- Identificação de ferramentas - No caso de grandes indústrias facilita o processo tanto de manutenção, como de substituição e administração das mesmas.

- Identificação de recipientes, embalagens e garrafas - Principalmente em produtos químicos e gases, onde um erro na hora de embalar pode causar danos sérios. Há possibilidades de identificação por exemplo de parâmetros como quantidades, peso, números de série, data, hora, etc. Em determinados casos este tipo de dados revelam-se fulcrais para o produto como em casos em que existe data de validade do mesmo. Estima-se que em relação ao código de barras, os operadores de armazém procedam a leitura das etiquetas aproximadamente 25 vezes, sendo que com RFID esse processo é automatizado revelando maior rapidez nos fluxos [36] (exemplo figuras 43 e 44).

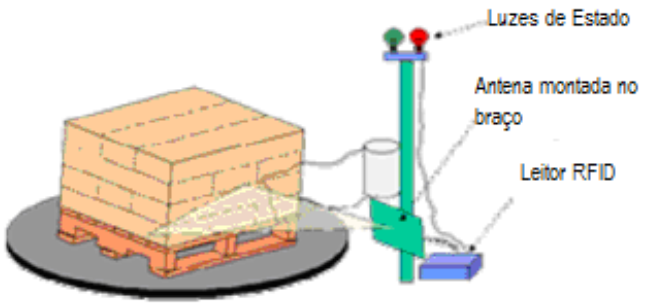


Figura 43 Aplicação em Empacotador

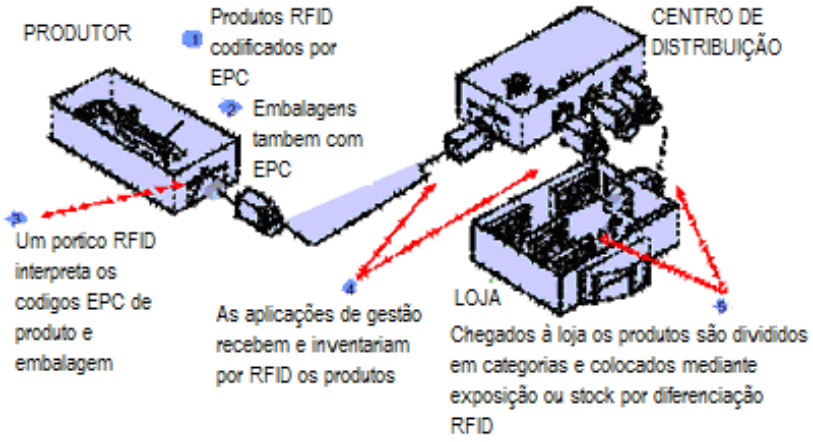


Figura 44 Aplicação do RFID a uma cadeia industrial

4.2.3 MANUTENÇÃO

As principais preocupações num processo de manutenção de sistemas complexos podem ser sumariadas em:

- Informações precisas e actuais sobre os objectos;
- Transferência em tempo real das informações dos incidentes críticos;
- Acesso rápido às bases de conhecimento necessárias para a solução do problema.

Um dos aspectos interessantes do RFID é a possibilidade de manter um histórico de manutenção no próprio objecto, melhorando, dessa forma, a sua manutibilidade.

Outro aspecto é a segurança, pois o RFID encontra-se embutido no objecto. Desta forma, as acções fraudulentas são coibidas de maneira mais eficaz. Como cada objecto possui um único RFID, não clonável, os prestadores de serviços não podem ludibriar os relatórios de manutenção, objectivando maiores ganhos financeiros. Como, por exemplo, relatando a troca de peças que não foram efectivamente trocadas.

O RFID ainda propícia uma melhoria na documentação do processo de manutenção, permitindo relatórios mais eficientes, além de uma redução dos custos administrativos em decorrência da diminuição da burocracia.

Devido à grande preocupação com uma manutenção ágil e eficiente, por exemplo, nas instalações aeroportuárias, o RFID torna-se uma alternativa proveitosa, já que provê facilidades para identificação, localização e monitorização de objectos físicos.

O aeroporto de Frankfurt (Franport), o segundo maior da Europa, com movimento superior a 50 milhões de passageiros por ano, iniciou um projecto-piloto em 2003 com o objectivo de testar os benefícios do RFID nas suas dependências. A manutenção no Franport é deveras exasperante, pois mais de 450 companhias são envolvidas no processo. Com o advento do RFID, o aeroporto começou a modernizar-se: os técnicos de manutenção agora usam dispositivos móveis para aceder aos planos de manutenção e registar as ordens de serviço. Todos os 22 mil extintores de incêndio foram equipados com RFID, identificando o histórico de manutenção, incluindo a última data de inspecção. Diariamente os técnicos percorrem o aeroporto efectuando as tarefas de manutenção necessárias. Para tal, os técnicos autenticam-se nos dispositivos móveis (usando também o RFID), recebendo as suas actividades do dia. Após o término de cada equipamento escalonado para inspecção, o técnico regista o seu RFID uma segunda vez, criando, assim, um registo de manutenção. Observando o caso de sucesso de Frankfurt, fica evidente que o RFID, de facto, pode optimizar os processos de manutenção. Conseguiu-se um ganho extraordinário de eficiência administrativa ao introduzir tal tecnologia nos extintores, uma tarefa que outrora consumira 88 mil páginas de papel que eram arquivadas por ano. Isso passou a ser feito de forma automática e com baixo custo.

Para a manutenção da infra-estrutura subterrânea do aeroporto de Atlanta, enterraram marcadores RFID que lhes permite identificar onde podem, por exemplo, encontrar cablagem. Justificou-se a entidade com o facto de aeroportos, de grande dimensão, serem ambientes dinâmicos e que, como tal, estão sujeitos a muitas remodelações, expansões, etc. Assim torna-se possível evitar possíveis erros e falhas de funcionamento derivado de, por exemplo, um cabo cortado. Desta forma evitam-se eventuais atrasos nas ligações aéreas ao serem prevenidos este tipo de falhas. Alternativamente a este novo sistema utilizavam-se, antes, marcadores de cimento de 130 kg, considerados muito inconvenientes pois exigiam muito mais trabalho para colocar e manter. Associada a este projecto esteve a empresa 3M que tratou de todo o processo relacionado com a tecnologia RFID.

4.2.4 IDENTIFICAÇÃO ANIMAL

Este tipo de sistema usado na identificação dos animais ajuda na gestão dos mesmos entre as empresas/quintas, no controlo de epidemias e garantia de qualidade e procedência [17]. A identificação animal por sistemas de RFID pode ser feita de quatro maneiras diferentes: colares, brincos, injectáveis ou ingeríveis.

- Os colares são fáceis de serem aplicados e transferidos de um animal para o outro; é usado geralmente apenas dentro de uma empresa.

- No caso dos brincos, são as *tags* de menor custo, e podem ser lidas a uma distância de até 1 m.

- No caso das *tags* injectáveis, que são usadas há cerca de 10 anos, ela é colocada sob a pele do animal com uma ferramenta especial, um aplicador parecido com uma injecção.

- A *tag* ingerível, ou *bolus* é um grande comprimido revestido geralmente por um material cerâmico resistente a ácido e de forma cilíndrica, que pode ficar no estômago do animal toda a vida. Regra geral, usam-se *tags* implantáveis por exemplo de vidro a baixa frequência (LF) porque são menos susceptíveis de atenuações provocadas por exemplo pela água e factores similares do que as *tags* de alta-frequência (UHF). Um nível avançado de uma instalação manipula dados de sensores conjuntamente com o RFID, reduzindo assim a acção humana nestas tarefas. Pode ser feito controlo de dosagens da alimentação e água de acordo com a temperatura, controla as falhas energéticas se ocorrerem [17].

Figura 45 Sistema RFID numa quinta [17]

4.2.5 COMERCIAL

- A **Wal-Mart** exigiu aos seus fornecedores que todos os produtos vendidos pela rede precisam conter etiquetas RFID. O grande impulsionador da tecnologia RFID, actualmente, tem instalado ou está em vias de atingir ¼ de lojas do grupo – composto por mais de 3 900 lojas – que utilizam o RFID para controlar o inventário. Estima-se que quando todo o sistema estiver completo a cadeia possa produzir aproximadamente 7 TB de dados RFID por dia [12]. Todo este processo esteve envolto em polémica, pois a Wal-Mart exigiu a muitos dos seus principais fornecedores que, não só colocassem *tags* ao nível da palete, como também do próprio produto. O retalhista esteve, durante o verão de 2006, a migrar as *tags* utilizadas da 1ª geração para *tags* Gen2. Os próprios fornecedores reconheceram a vantagem competitiva, comercial e enorme potencial do RFID e estão, eles mesmos, a implementar os seus sistemas. A utilização da tecnologia, para determinar outro tipo de informação acerca dos produtos, está também a ser equacionada. Quer para determinar as temperaturas às quais se encontram os produtos – prevenindo assim uma eventual degradação destes devido a más condições de armazenamento - quer também para ter informação centralizada nas suas aplicações sobre datas de validade de lotes e produtos, de forma a escoar aqueles com prazos inferiores. O tempo necessário para realizar um inventário reduziu das quatro horas para os 45 minutos, fruto da colocação de *tags* activas nos veículos que efectuavam entregas [39].

- Um supermercado na pequena cidade alemã de Rheinberg/Dusseldorf, disponibiliza aos moradores que fazem as suas compras o uso de carrinhos equipados com um assistente de compras pessoal (figura 46), que nada mais é do que um computador. Diversos produtos disponíveis nas prateleiras — como lâminas de barbear, champôs, queijos, CD e DVD — trazem etiquetas inteligentes na embalagem. À medida que esses itens são colocados no carrinho, as *tags* emitem sinais de rádio informando o seu código, ao qual o sistema da loja associa o preço. Tudo é somado e exibido na tela do assistente de compras. No final, basta fazer o pagamento. Alem disso as prateleiras também são inteligentes. Por meio dos leitores RFID espalhados pela loja, uma prateleira "avisa" o sistema que, por exemplo, restam apenas duas embalagens de uma marca de leite. Da sua sala, o gerente manda um alerta para um

funcionário determinando a reposição imediata. Também dá para monitorizar a data de validade dos produtos à venda — gravada nas *tags* — e, se ela estiver próxima do final, colocar o item imediatamente em promoção.

Figura 46 Personal Shopping Assistant colocado num carrinho de compras

Este pequeno computador dispõe de um *touchscreen*, à semelhança dos dispositivos Pocket PC, e de um leitor de códigos de barras. É acoplado ao carrinho de compras quando o cliente inicia a sua visita à loja [39].

- Na vanguarda em Portugal encontra-se a Throttleman, empresa portuguesa de produção têxtil. O projecto envolve toda a linha de produção da marca têxtil, desde a produção de etiquetas à colocação das mesmas. O objectivo é contabilizar de forma automática os itens quando chegam ao armazém. Informação em tempo real, aumento da fiabilidade e velocidade de inventário, contagem e validação de itens sem abertura de caixas, capacidade de conferir, e leitura de 15 mil peças por hora, destacam-se entre as vantagens da tecnologia. A solução está dividida em três áreas: a *Edgeware* é a camada física da tecnologia, composta pelas *tags* passivas, leitores manuais, entre outros. A segunda área é a Integração, responsável pela gestão e filtragem de informação e integração da mesma com a camada operacional. Por último, a solução *RetailID*, que agrega a gestão, o controlo e a rastreabilidade dos artigos. No final de 2008 deverá chegar também às lojas da marca o *Magic Mirror* (figura 47). Este espelho mágico será colocado nos provadores de cada loja e será capaz de ler as *tags* RFID colocadas nas peças de roupa que cada cliente está a experimentar, a partir daí o utilizador terá à sua disponibilidade várias funcionalidades disponibilizadas através do *touchscreen* lançado no espelho mágico. Uma das funcionalidades será o cliente poder seleccionar outro tamanho da peça de roupa que está a experimentar, efectuando

assim um pedido que segue directamente para um dispositivo de um funcionário [25].

Figura 47 Espelho Mágico

O Magic Mirror é um novo canal de *merchandising*, permitindo disponibilizar, em simultâneo, imagens de outras peças de roupa que condizem com a que está a experimentar. O eventual pedido poderá ser feito também através do *touchscreen*.

4.2.6 SERVIÇOS E PRODUTOS PARA O CONSUMIDOR

E porque não ter um frigorifico inteligente, por exemplo, equipado com leitor RFID, que terá condições de verificar o seu próprio conteúdo, com base nas informações transmitidas pelas *tags* dos produtos guardados dentro dela — uma caixa de leite, um iogurte, um frasco de azeitonas? À medida que esses produtos são retirados do interior, a informação pode ir, via web, para uma lista de compras armazenada num PDA ou até mesmo directo para o supermercado.

Este é somente um dos serviços que o consumidor poderá vir a utilizar no curto prazo, alguns deles estão já em fase de implementação.

4.2.7 BIBLIOTECAS

Em bibliotecas e centros de informação, a tecnologia RFID é utilizada para identificação do livro, possibilitando leitura e rastreabilidade dos exemplares físicos das obras.

Funciona fixando uma etiqueta de RFID (*tag*) plana (de 1 a 2 mm), adesiva, de dimensões reduzidas (50 x 50 mm em média), que contem no centro um *microchip* e à volta deste uma antena metálica em espiral, com um conjunto de sensores especiais e dispositivos fixos

(portais), de mesa ou portáteis (manuais) que possibilitam a codificação e leitura dos dados dos livros na mesma, principalmente o seu código identificador - antes registado em códigos de barras.

A etiqueta é inserida normalmente na contracapa dos livros, perto da lombada, dentro de revistas e sobre materiais multimédia (CD-ROM, DVD) para ser lida à distância.

É possível converter facilmente os códigos identificadores existentes actualmente, no código de barras para etiquetas RFID, através de equipamentos próprios para esta conversão.

4.2.8 ANTI-ROUBOS

Além do controlo de acesso, um sistema RFID pode fornecer na área de segurança outros serviços. Um deles: os sistemas de imobilização.

No início dos anos 90 o roubo de carros subiu, tornando o mercado de segurança para carros, alarmes e sistemas de imobilização, um mercado promissor. Os controlos de alarme com alcance de 5 a 20 m estão no mercado há anos, e são pequenos transmissores de rádio frequência que operam na frequência de 433,92 MHz. Neste tipo de sistema de segurança para carros, é somente este controlo que pode accionar o destrancar do carro, permitindo que ele seja aberto sem que um ruído seja emitido. Permitir que o carro possa ser ligado é trabalho do sistema de imobilização. O problema é que, se o controlo que o destranca for violado, o carro ainda assim pode ser aberto através das chaves, por um processo mecânico, mas não há como o sistema reconhecer se a chave inserida é genuína, permitindo que uma ferramenta específica ou uma chave-mestra possa abrir o veículo. A tecnologia dos *transponders* de RFID podem agir justamente neste ponto, verificando a autenticidade da chave, assim o sistema antigo cuida do alarme e de destrancar, e a *tag* RFID da imobilização. Assim, se uma chave que não for a original do carro tentar ligá-lo, o carro é então imobilizado, mesmo que o alarme tenha sido desligado e as portas abertas. Mobilização Electrónica é o nome dado a este sistema, onde o sistema de ignição é combinado com um *transponder*, incorporado directamente no topo da chave [3].

Também para a localização de bens móveis, onde a designação comum é RTLS – *Real Time Location Systems*, ou Sistemas de Localização em Tempo Real.

Estes sistemas usam *tags* activas que, não sujeitas a fonte exterior de radiofrequência, emitem de modo próprio o seu ID para antenas receptoras colocadas na zona de supervisão do sistema. Os sistemas permitem que, a qualquer instante, se conheça a presença e a localização dos bens supervisionados (bens onde está colocado um *tag* RTLS).

A localização dos bens é possível porque as antenas, ao receber o sinal do *tag* activo com um ID específico, e antes de enviarem a informação para o servidor central do sistema, adicionam ao pacote de informação enviado, a hora de recepção do sinal do *tag*.

Assim sendo, e por comparação da hora a que o sinal de um dado *tag* é recebido em três ou mais antenas do sistema, é possível por triangulação conhecer a localização exacta deste e consequentemente do bem que o transporta.

4.2.9 PASSAPORTES

Iniciou-se a emissão de passaportes com *chip* RFID. O principal objectivo é controlar as entradas e saídas de um país. Além do identificador unívoco de cada *chip* poderão ser associados ao portador do passaporte outros dados extra, como por exemplo: o nome, uma foto digitalizada, impressões digitais e até mesmo cartões de crédito virtuais. O principal objectivo da utilização desta tecnologia nos passaportes é o de evitar que sejam feitas falsificações nas páginas escritas, pois os dados contidos no *chip* são uma cópia exacta daquilo que é visível nas suas páginas. No entanto exige-se que estes documentos de identificação tenham um prazo de validade bastante alargado, tipicamente de 10 anos, e em termos de segurança informática existe pleno conhecimento que muito dificilmente uma tecnologia, como é o RFID, poderá oferecer mecanismos de segurança viáveis a longo prazo. É, efectivamente, um grande risco pois alguém que coleccione informação destes *chips* poderá possuir conhecimentos que lhe permitam reproduzir ou alterar os dados durante esse prazo temporal.

Tambem na União Europeia se fala do uso dos passaportes biométricos. São dotados de um *chip* RFID que, além da identificação do portador (nome, filiação, data e país de nascimento) contem, inicialmente, a foto digitalizada e dados faciais (um conjunto de números, que representam uma intrincada relação entre parâmetros característicos do rosto humano – como distâncias e ângulos entre olhos, boca, nariz, maçãs faciais – e outros

dados antropométricos usados por uma tecnologia de identificação denominada reconhecimento de fisionomia. Dentro de pouco tempo, o *chip* conterá também a impressão digital digitalizada.

4.2.10 CARTÕES DE CRÉDITO

As principais empresas emissoras de cartões bancários estão também a aderir, em massa, ao RFID. As aplicações encontradas, até ao momento, foram em termos de segurança e criação de uma nova forma de pagamento de serviços e produtos.

- A American Express, afirma que é possível realizar um pagamento em apenas 2 s. Estatísticas calculadas após um teste-piloto provaram que é possível atingir melhorias de 63% relativamente a pagamentos em dinheiro e de 53% quando comparado com os pagamentos Multibanco tradicionais. O objectivo da empresa é o de disponibilizar este sistema a todas as lojas de conveniência, restaurantes de *fast-food*, supermercados, farmácias e bombas de gasolina. Efectivamente, este serviço destina-se a pagamentos de serviços ou produtos que não envolvam valores avultados, visto não ser necessária qualquer tipo de identificação – basta acenar o cartão pelo dispositivo receptor.

- A MasterCard dispõe de um cartão de crédito utilizando tanto o *chip* tradicional – conjuntamente com PIN – como a tecnologia RFID, permitindo assim pagamentos sem ter que efectuar qualquer tipo de contacto entre o cartão e os dispositivos leitores. A MasterCard espera que este método de pagamento tenha sucesso em locais onde a velocidade de transferência seja um factor determinante (/e.g./ restaurantes, portagens, etc.).

- A VISA já disponibiliza este tipo de cartões que permite aos consumidores efectuar pequenos pagamentos de forma rápida e sem colocar em risco o seu cartão – contra tentativas de duplicação e apropriação indevida do seu PIN. O cartão, à semelhança das alternativas dos seus concorrentes, funciona a distâncias muito pequenas do leitor – cerca de 10 cm. Há ainda uma outra inovação que dá pelo nome de ***Visa payWave*** e permite ser usado como um porta-chaves**.** Para pagamentos inferiores a 25 € não é necessária uma assinatura do utilizador o que facilita e acelera o acto de pequenas transacções (figura 48) [39].

Figura 48 Micro Tag da Visa [39]

A tecnologia usada neste porta-chaves é muito semelhante à tecnologia ***PayPass*** da MasterCard. A VISA garante segurança máxima neste dispositivo devido às seguintes características:

• Leitura do dispositivo é possível apenas através do encosto deste a um *reader*;

• Para cada transacção é criada uma chave única que é enviada para a rede VISA;

• Estas *tags* passivas não contêm o número de conta do utilizador, apenas possuem o logo da VISA.

4.2.11 ESCOLAS

Na capital de Taiwan, Taipé, a escola primária de Nan Hu decidiu adoptar novas tecnologias para fornecer segurança aos seus alunos dentro dos domínios da escola, acarretando com todas as responsabilidades que isso traz, já que se trata do bem-estar dos alunos. Em adição à implementação de um sistema via Internet que permite a professores e pais manterem registo das faltas dos alunos, a direcção da escola decidiu ser a primeira a nível mundial a implementar um sistema de RFID para controlar as entradas e saídas da propriedade da escola. Presentemente, cada um dos 65 alunos dos 4 níveis de ensino da escola está equipado com uma *tag* activa, que contém os seus dados de aluno, que pode ser usada por cima da roupa. À entrada da escola, foi colocado um sensor RFID que detecta se o aluno entra ou sai da área da escola e, com os seus dados inseridos na *tag*, compara-os com a base de dados de alunos e informa o docente da situação do aluno, através do envio de uma SMS, melhorando significativamente a gestão das presenças. Foram também instalados sensores RFID em áreas potencialmente perigosas, que não possuem supervisão

do pessoal escolar, de modo a que na eventualidade de um aluno lá entrar, o sistema alerte imediatamente os docentes e o pessoal de segurança através de SMS.

Com todos os dados retirados do projecto, é também futuramente possível calcular informação estatística sobre o comportamento dos alunos, de modo a planear futuras melhorias não só a nível do próprio ensino, mas também a nível da instituição em si, nomeadamente em outras medidas de segurança. O objectivo actual é atingir a estabilidade de todo o sistema e torná-lo mais diversificado, por exemplo, fornecendo PDA ou *readers* manuais aos seguranças e equipando os computadores com sistemas de notificação mais eficazes e avançados.

4.2.12 CHIPS NOS VEÍCULOS EM PORTUGAL

Com a Via Verde quem circula pelas estradas pode usar o RFID para passar por um ponto de pagamento ou controlo sem precisar parar o carro. Instalada no vidro do veículo, a etiqueta inteligente guarda a sua identificação e a categoria à qual pertence — que servem de base para a posterior cobrança, enviada para casa. A *tag* activa tem uma bateria embutida que lhe garante um tempo de resposta curto — cerca de 30 milissegundos. Os leitores no caso da Via Verde estão dispostos nas passagens das portagens.

O sistema baseia-se numa Base de Dados Central (figura 49), localizada na Via Verde Portugal, que está ligada a todas as portagens e à SIBS – Sociedade Interbancária de Serviços, S.A.

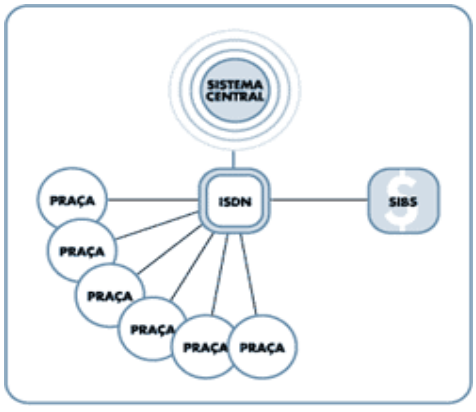


Figura 49 Sistema Central Via Verde [41]

Os dados fornecidos pelo cliente, são inseridos na Base de Dados Via Verde Portugal (figura 50). A identificação do cliente é então enviada para a SIBS.

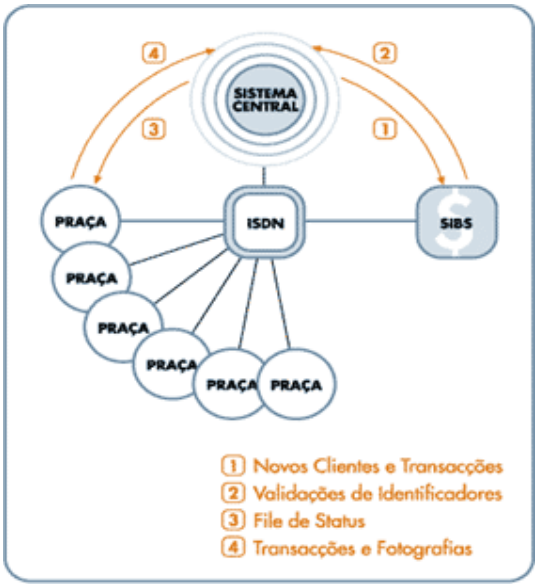


Figura 50 Troca das Informações [41]

Diariamente, é criada uma lista de todos os identificadores que estão associados a contas bancárias, a chamada *status file*, que é enviada para todas as portagens. É condição necessária, o identificador constar nesta lista, para que se acenda o semáforo verde na passagem pela Via Verde.

Acrescente-se que, no caso de mais tarde haver algum problema com o cartão multibanco usado na associação à conta bancária, a SIBS informa a Via Verde Portugal da situação, e o identificador é retirado da *status file*.

Ao entrar numa Auto-estrada (figura 51) em sistema fechado, onde a taxa de portagem depende da classe do veículo e do local de entrada, a antena localizada na via escreve no identificador a informação relativa à entrada:

- Portagem de entrada

- Via de entrada

- Hora de entrada

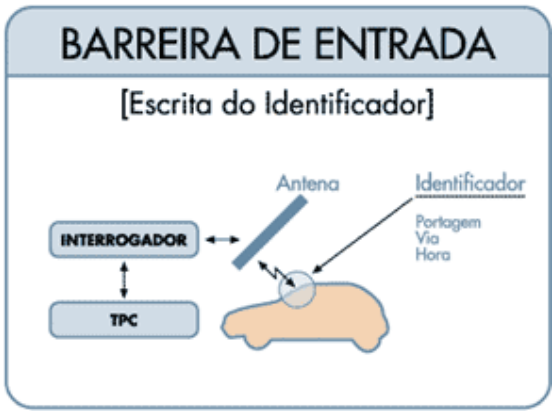


Figura 51 Sinais da entrada na Portagem [41]

Ao sair da auto-estrada (figura 52), a antena localizada na via lê do identificador os seguintes dados:

- Portagem de entrada

- Via de entrada

- Hora de entrada

- Número do identificador

- Classe do identificador

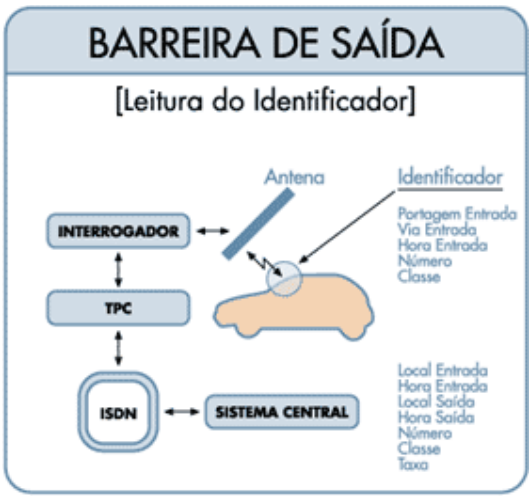


Figura 52 Sinais da Saída na Portagem [41]

De notar que, no caso das portagens em sistema aberto, onde a taxa de portagem depende apenas da classe do veículo, como é o caso das pontes sobre o Tejo, a informação da transacção depende apenas de um único evento – a passagem pela antena.

Para a constituição de uma transacção completa, são ainda usadas as informações da *status file* e de um equipamento que classifica o veiculo à passagem pela via, de forma a confirmar a classe do identificador instalado.

Se todos os dados estiverem correctos, o valor da transacção é calculado e exibido no ecrã externo da portagem, ao mesmo tempo que se acende o semáforo verde. Caso seja verificada alguma anomalia, ou irregularidade, acende-se o semáforo amarelo e é tirada uma fotografia para análise.

As transacções e fotografias ficam armazenadas no computador da portagem, sendo transferidas para o Sistema Central da Via Verde Portugal, várias vezes por dia, e importadas para a Base de Dados.

Todos os dias, é criado um ficheiro para cada concessionária, com as transações geradas nas respectivas portagens, que depois é enviado para a SIBS. As taxas das transacções, identificadas pelo número do identificador, são então debitadas na conta bancária do cliente e creditadas na conta bancária da concessionária.

Na Europa, no Canadá e no Chile já existem pontos de controlo, que permitem rodar a até 160 km/h com esse sistema. A frequência utilizada está na casa dos 5,8 GHz.

Complementar à Via Verde em Portugal (tecnologicamente igual com a diferença que os leitores também serão agora móveis) a polícia vai saber se o seguro e a inspecção estão em falta. Um *chip* onde consta informação sobre o seguro automóvel e a inspecção periódica vai passar a ser obrigatório. O dispositivo permitirá decisões mais sustentadas sobre quais os melhores investimentos em infra-estruturas rodoviárias, tal como uma gestão do fluxo de tráfego nas principais vias, possibilitando o aconselhamento, em caso de congestionamento, de roteiros alternativos. Além da fluidez de tráfego, o *chip* também ajudará a decidir a construção de novas estradas com evidência científica. Pode saber-se quantos carros passam em determinada zona. A possibilidade de sobre este dispositivo se desenvolverem serviços como a cobrança electrónica de portagens vai também ao encontro de objectivos de protecção ambiental e de poupança de combustíveis, uma vez que a

redução das paragens para o pagamento de portagens reduz o consumo de combustíveis e a consequente emissão de gases de escape.

Há quem defenda que este sistema parece ser inútil, até prejudicial, do ponto de vista da facilitação da vida do utente; o governo, e os seus parceiros privados neste projecto, passam a deter um poder excessivo e injustificado para controlar, e eventualmente taxar, os veículos; o direito à privacidade dos automobilistas é posto em causa. Há até quem já lhe chame o novo *Big Brother* (figura 53).

Figura 53 O novo "Big Brother" de RFID

5. IMPLEMENTAÇÃO

5.1 DESENVOLVIMENTO DO PROJECTO RFID

A intenção do progresso deste projecto consistia (como foi referenciado na introdução) em fazer-se um sistema que colmatasse algumas lacunas existentes no espaço da Academia de Formação ATEC. Esta é composta por cerca de 200 activos colaborantes repartidos entre formandos, formadores e funcionários internos (administração, consultoria, formação interna). O objectivo final era o de ter um sistema que fizesse o controlo de acessos completo destes activos, portanto registando as suas entradas e saídas ao pormenor. Deveria ainda após o registo, ficar um arquivo com todos os apontamentos de acessos para posterior consulta, e respectiva parametrização como por exemplo: processamento de salários, registos de assiduidade e pontualidade, e presença nas instalações. Para a estruturação do projecto foram definidas algumas etapas importantes respeitantes à gestão de tarefas. A figura 54 demonstra as variáveis a levar em conta para estruturar e planificar o processo de desenvolvimento de um sistema baseado em RFID.

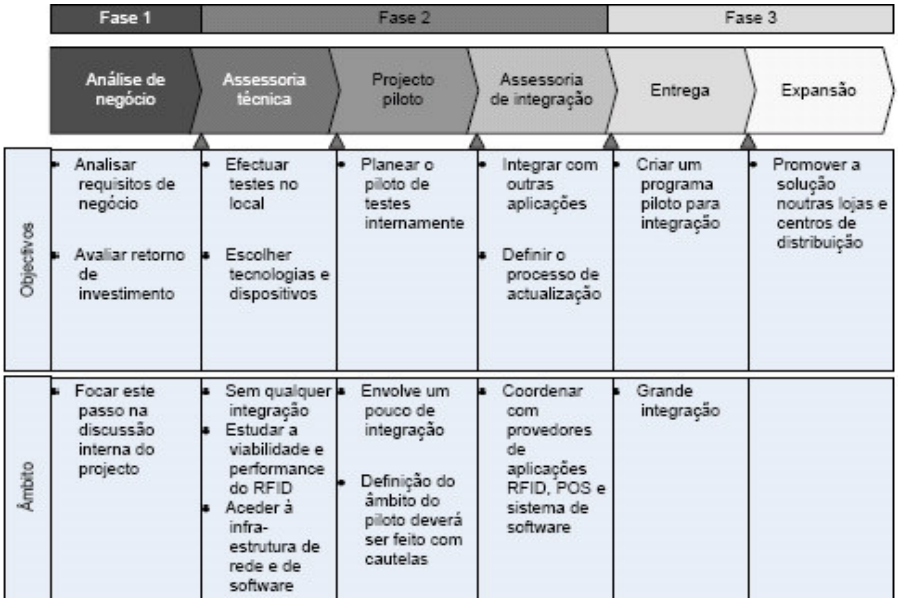


Figura 54 Fases Essenciais de desenvolvimento de um Projecto RFID [33]

Como é possível constatar, são definidas 3 fases principais, à semelhança de um projecto de desenvolvimento genérico de um sistema de informação, em que na primeira deverá ser feita a análise de requisitos e estudo de caso do negócio; na segunda especificar e desenhar o sistema para depois tratar do desenvolvimento; e finalmente a fase de implementação. A utilização destas fases para implementação de um sistema RFID pretende aumentar as hipóteses de êxito do projecto.

- ANÁLISE DE REQUISITO E ASSESSORIA TÉCNICA

Nesta fase devem ser analisados os requisitos de negócio e quantificar os retornos do investimento. A escolha das tecnologias e dispositivos será também feita nesta fase. Todos estes passos auxiliam no conhecimento da tecnologia RFID.

- CASO DE TESTE E ASSESSORIA DE INTEGRAÇÃO

Na segunda fase é necessário planear um piloto, para testes, interno que consiga demonstrar valor, benefício, risco e potencial retorno de investimento que advêm da utilização do RFID. Este piloto deverá cobrir a maioria dos domínios necessários e processos genéricos.

- ENTREGA E PROMOÇÃO

Finalmente, na terceira fase, dever-se-á proceder à integração, do piloto construído na fase anterior. Se tudo correr em conformidade com o esperado inicia-se a promoção da solução junto dos utilizadores [39].

Dada a complexidade inerente houve a necessidade de subdividir em múltiplas tarefas de realização mais simples (explicitadas na calendarização), tais como:

- Possibilidades de concretização e integração;
- Definição de parâmetros concretos e de execução;
- Reuniões com as empresas para a escolha do equipamento;
- Escolha de equipamento;
- Desenvolvimento Software em Visual Basic, VBA e Access.

Ao longo do desenvolvimento pretende-se expor todas as fases da execução do Estágio e serão apresentadas todas as etapas de decisão e de actuação para que se possa perceber melhor a temporização de cada uma delas, ao mesmo tempo que se pretende que possa também ser útil para futuras decisões de âmbito semelhante.

Todas as fases que, como é óbvio implicaram decisões, nalguns casos de âmbito profundo, foram sempre devidamente contempladas do ponto de vista dos coordenadores, do executante e acima de tudo, do ponto de vista que melhor representasse a empresa em todos os parâmetros possíveis.

No que diz respeito à programação do dispositivo, é feita uma abordagem global pelos pontos essenciais da mesma. Todos os passos e rotinas têm a devida explicação que se pensa poderem dissipar dúvidas em áreas específicas da mesma (entregues com o CD do estágio).

5.2 EXECUÇÃO

5.2.1 DEFINIÇÕES

As bases estruturais de todo o sistema são as validações. O que se pretende são unidades de leitura (*readers*) espalhadas por toda a Academia (nomeadamente uma em cada sala) para que o utilizador possa em qualquer momento fazer uma entrada ou saída do sistema.

Sendo assim a estrutura base do sistema assenta sobre algo semelhante ao exposto na figura 55.

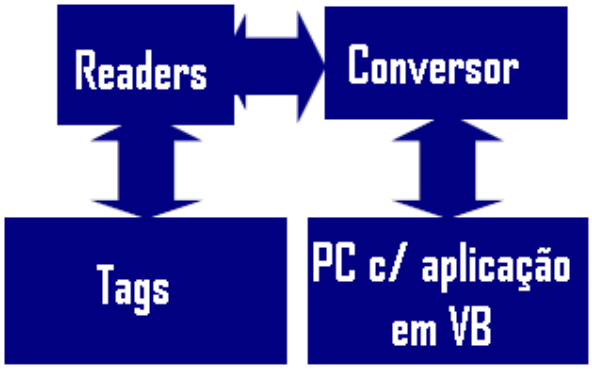


Figura 55 Blocos Estruturais do Sistema desenvolvido [33]

Com um cartão ou um porta-chaves definem-se as etiquetas. *Tags* estas postas em frente do *reader* (equipamento escolhido no estudo) que transmitem informação necessária ao acesso em questão. Após o sinal da etiqueta ter sido recebido pelo leitor essa informação é recolhida, desencriptada e transformada num protocolo de comunicação que, regra geral, é *wiegand*. Esta é a fase do *middleware*. Por último, a informação para ser adquirida pelo PC tem de ser novamente convertida (pelo conversor) para um protocolo conhecido, como por exemplo RS-232 ou RS-485. Após a entrada da informação no PC esta pode ser tratada e arquivada mediante o software que se pretenda, que neste caso será Microsoft VB, VBA (Visual Basic) e Microsoft Access.

Estes são os componentes essenciais do sistema, e a forma como eles se interligam.

Para que o hardware pudesse ser adquirido procedeu-se a uma análise do que existia no mercado.

5.2.2 ANÁLISE DE MERCADO (HARDWARE)

Foi então necessário proceder-se a uma procura exaustiva no mercado de empresas, que estivessem directa ou indirectamente relacionadas com este tipo de projectos. De entre estas empresas, há de imediato três que se destacam pela qualidade de resposta dada, através das quais foi estabelecido contacto e foram pedidos orçamentos e previsões para a possível execução.

5.2.2.1 TELEMAX

Bastante implementada no Porto em termos de serviços e vendas de equipamentos pareceu logo à partida ser uma boa solução pela disponibilidade dos intervenientes. Prontamente se dispuseram a fazer uma reunião nas instalações da ATEC para ser formada uma opinião acerca do equipamento a utilizar, além de, sem requisição, se oferecerem a fornecer tudo o que fosse necessário à concretização do projecto em termos de *hardware* e de *software*. Com uma gama bastante interessante de produtos assim como com uma variedade de serviços, apresentou aquela que acabou por ser, como explicitado no estudo de custos, a melhor proposta para a execução do projecto.

5.2.2.2 NETPONTO

Também implementada no Porto, esta empresa é o espelho de uma organização vocacionada para o sucesso. Com instalações e pessoal extremamente eficazes, afirmou-se com grande notoriedade até pelo tipo de serviços já executados, donde se destacam uma boa lista de empresas e/ou organizações públicas e privadas. Com um equipamento aparentemente bom, e agradável em termos funcionais, esta empresa acabou por não ser escolhida devido à sua forma de operar mais fechada no que diz respeito à abordagem para este tipo de iniciativas. Não se apresentaram tão disponíveis como seria de esperar, o que resultou no final por uma menor quotação para a escolha. Com um estudo de custos muito próximo do apresentado pela anterior empresa, acabou como citado por não prevalecer devido ao seu *modus operandi* mais reservado em fornecimento de *hardware* (para testes) e de *software* (o SDK para comunicação com os equipamentos).

5.2.2.3 BIOGLOBAL

Implementada em Lisboa e por isso logo à partida com um *handicap* de comunicação relativamente à localização, e com uma eficácia menos conseguida, esta empresa também se destaca em termos de mercado pela sua reputação em instalação deste tipo de projectos. Menos célere do que se desejaria, apresentou uma proposta demasiado ponderada e mais na perspectiva da venda do equipamento e do serviço como um pacote, do que propriamente como colaboradora de um projecto desta génese, apesar de todos os factores e condicionantes terem sido devidamente explicitados de antemão. O estudo de custos

pareceu ser exagerado em termos globais e ficou a surpresa da pouca disponibilidade para colaboração. Posta de lado à partida por todas estas condicionantes.

Pela disparidade de factores e como já explicado acima destacou-se pela positiva em quase todos os parâmetros a empresa Telemax, que assim foi a escolhida para a estreita colaboração tida no desenrolar de todo o processo. Mediante acordo e requisição foi então disponibilizado o *hardware* para utilização a termo, assim como o *software* de comunicação com o mesmo equipamento, com a vantagem/curiosidade de ter sido dito que as rotinas do mesmo (SDK – *software* de comunicação) poderiam, sem qualquer tipo de problema, ser utilizadas no desenvolvimento do sistema, o que acabou por se revelar francamente positivo pois facilitou a abordagem ao equipamento. Foi ainda fornecido um *software* "fechado" de Gestão de Assiduidades para comparar com uma possível solução a adoptar de futuro.

O resultado final desta colaboração revelou-se como francamente positivo pelos resultados obtidos entre as partes.

5.2.3 HARDWARE

De forma a serem escolhidos então os leitores a as etiquetas foi realizada uma comparação de equipamentos dentro da realidade da empresa Telemax. Existiam então quatro opções de aquisição.

5.2.3.1 PRIMEIRA OPÇÃO

Nesta primeira abordagem o equipamento em causa era identificado por IP505R (*master*) que permitia uma ligação em lógica *Master-Slave* com um outro identificado por IP10 (*slave*) ligados por cada duas salas da Academia. A lógica *Master-Slave* baseia-se na existência de um equipamento principal para vários equipamentos auxiliares, como se representa na figura 56. Na lógica da implementação em 12 salas teriam que ser então instalados 6 equipamentos *Master* IP505R e 6 equipamentos IP10, porque cada *Master* só suporta um *slave*. Em termos de software havia em todos os aspectos compatibilidade com o desenvolvimento feito em Visual Basic e Access. Entre os IP505R o protocolo utilizado é o RS-422 que tem de ser convertido depois em RS-232. Entre *master* e *slave* o protocolo

utilizado é o *wiegand* pois o IP10 utiliza ou *wiegand* ou RS-232, mas como, o *master* tem uma entrada de dados *wiegand*, estes ligam-se desta forma.

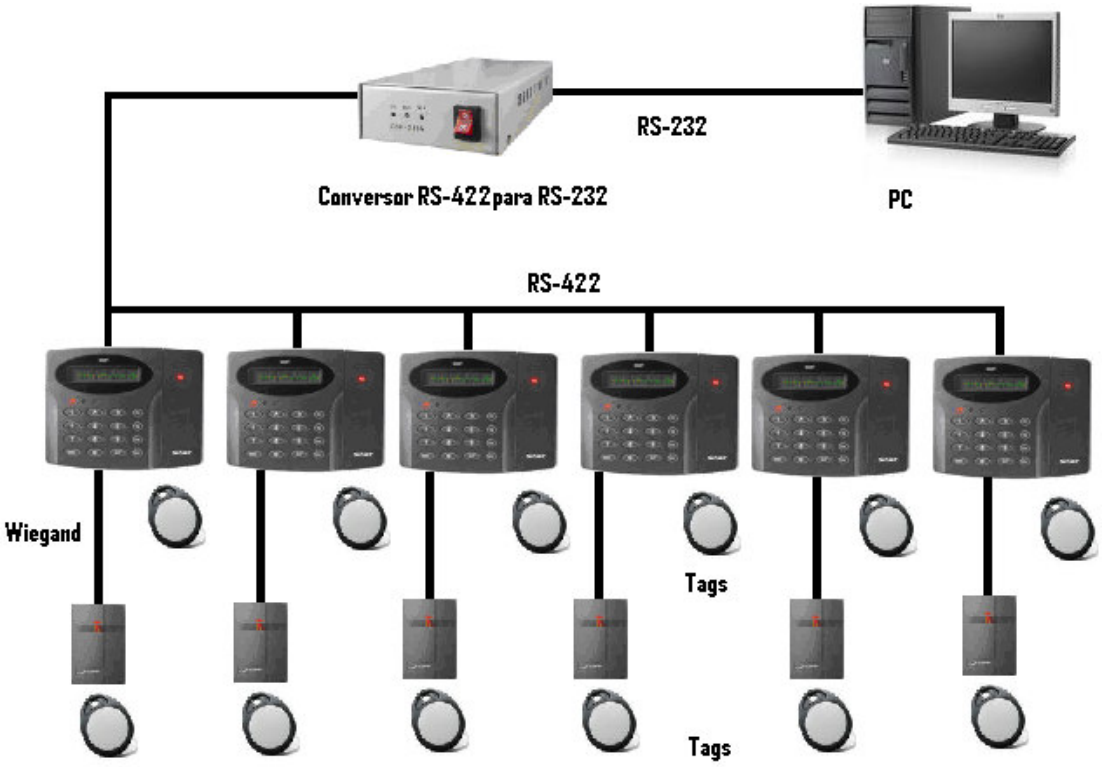


Figura 56 Esquema da Primeira Opção

Em termos de custos esta solução teria um custo unitário do IP505R de 315 € + IVA e do IP10 de 48 € + IVA. Há ainda que adicionar o preço do conversor que é de 54 € + IVA. O que perfazia um custo total de 2680 €.

Descrição dos Equipamentos

Figura 57 IP-505R

As características deste equipamento são:

- Reconhecimento de RFID com codificação PSK de 128 bits a 125 khz e Pin;

- Controlo dinâmico de 10 000 ID e 7 250 eventos;

- Comunicação série via RS-232, RS-422 ou RS-485 (max 32 canais);

- Porta para leitor externo para funcionamento em modo Anti-Passback: Wiegand 26 bit;

- Microprocessador 32 bit ARM e DUAL 8 bit;

- Memória do programa 128 kB Flash;

- Memória de dados 128 kB / 256 kB / 512 KB Flash;

- LCD com 2 linhas de 16 caracteres;

- Teclado numérico com 16 teclas retroiluminadas;

Figura 58 IP-10

As características do IP10 são:

- Leitor proximidade a 13,56 MHz;

- Área de alcance até 10 cm;

- Saída 34 bit Wiegand, opcional como RS-232;

- Porta RS-232 de comunicação para função de leitura e gravação;

- Área de alcance até 10 cm

- 100% à prova de água

- Leitor de cartões / tags activos e passivos

5.2.3.2 SEGUNDA OPÇÃO

Esta vertente revelou-se interessante pela equivalência também em termos de *software* (igual SDK) e pela grande capacidade dos equipamentos utilizados. A proposta passaria por aplicar 12 dispositivos IP505R (figura 57), que têm conforme o descritivo acima imensas funcionalidades, de onde se destacam os 10 000 activos identificáveis e o registo de 7 250 eventos (figura 59).

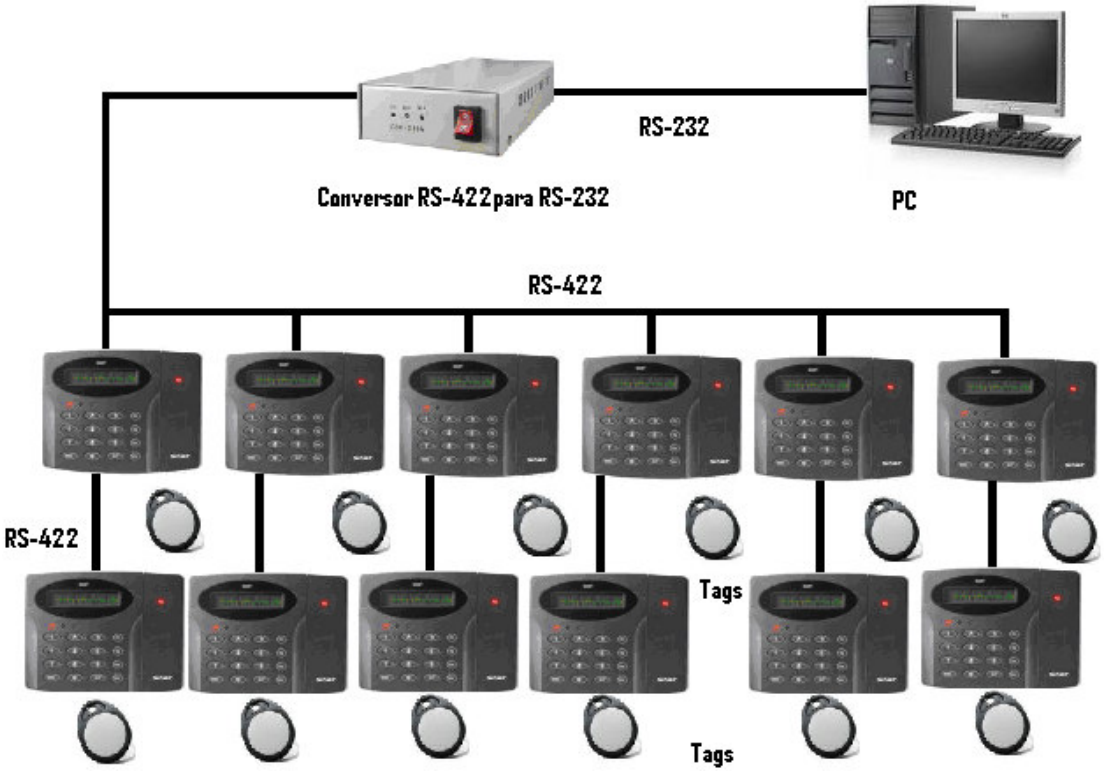


Figura 59 Esquema da Segunda Opção

O preço desta solução seria então de 315 € + IVA por cada IP505R adicionado ainda o valor do conversor de 54 € + IVA, o que totalizava 4600 €, o que se revelou desanimador face ao exagero de gasto só na aquisição de *hardware.*

5.2.3.3 TERCEIRA OPÇÃO

Esta opção (figura 60) implicava a aquisição de três armários ITDC *Pack* 1 que albergava a concentração das ligações de 12 dispositivos IP10. Esta solução revelava-se extremamente profissional pela escolha do equipamento em si (ver descritivo). Para uma organização que tenha grandes pretensões de controlo de acessos esta parece ser a solução mais completa, pois permite o registo de 50 000 utilizadores e a memorização de 29 500 eventos sem que tenha de estar ligado à unidade central. Tem ainda a vantagem de possuir uma bateria de *backup* para o caso de haver alguma inesperada interrupção do fornecimento de energia eléctrica. No entanto o custo de aquisição revelou-se mais uma vez decisivo face à tecnologia empregue.

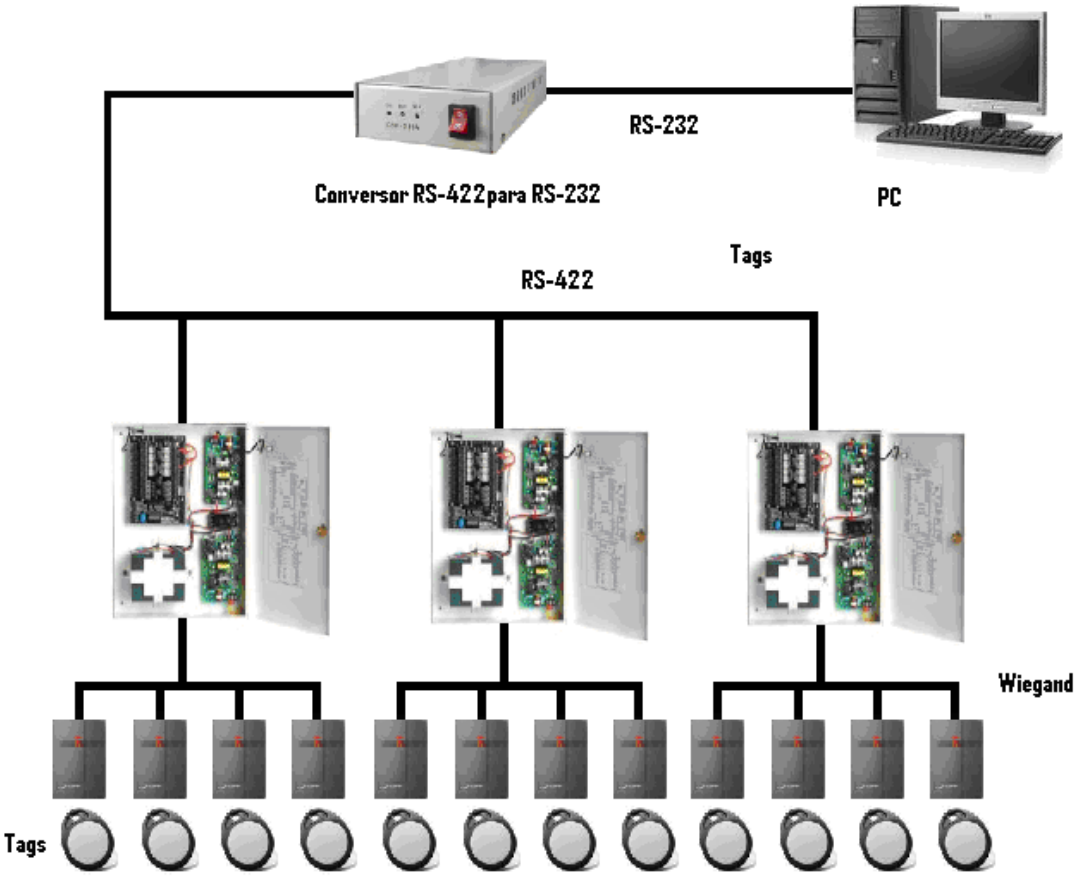


Figura 60 Esquema da Terceira Opção

Os custos seriam então de 665 € + IVA por cada ITDC e de 48 € + IVA por cada IP10, adicionando ainda o preço do conversor (54 € + IVA) que somados resultavam em 3154 €.

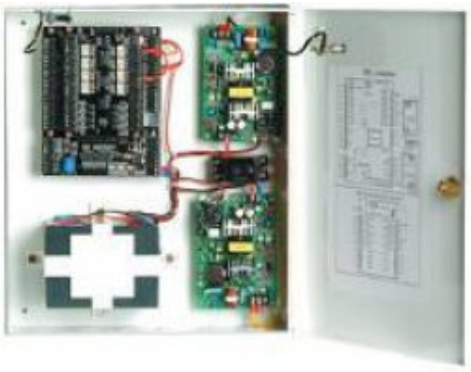


Figura 61 iTDC

As características deste equipamento são:

- Painel de Controlo de Acessos Profissional para 4 leitores;

- Controlo dinâmico de 50 000 IDs e 29 500 eventos;

- Comunicação série via RS-232, RS-422 ou RS-485 (max 256 canais);

- 4 Portas para leitores externos para funcionamento em 2, 3 ou 4 portas: *Wiegand* 26 bit;

- Possibilidade de comunicação por *Ethernet* (TCP/IP).

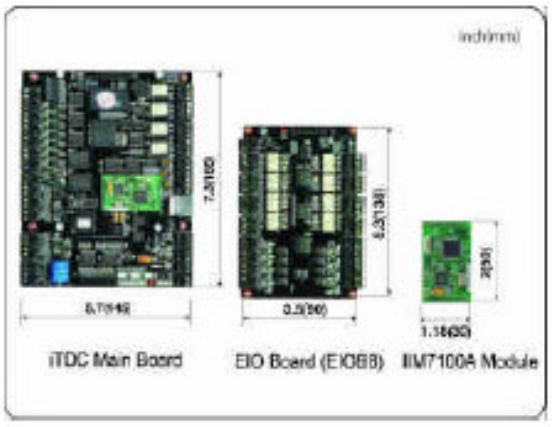


Figura 62 Placas Internas do iTDC

O equipamento IP10 já foi descrito na primeira opção e neste caso o *software* já desenvolvido teria de ser alterado para o SDK de comunicação deste equipamento.

5.2.3.4 QUARTA OPÇÃO

A quarta e última alternativa revelou-se a mais interessante e adequada à empresa. Apresenta a desvantagem de não ter um *software* de comunicação compatível com a maior parte dos desenvolvimentos já realizados, mas facilmente adaptável. A maior vantagem assume-se pela sua instalação em termos de cablagem pois são necessários bastante menos cabos que nas anteriores soluções, e isso também é um custo. A comunicação faz-se entre os leitores por RS-485 (protocolo-norma que permite a comunicação em série de vários dispositivos) que tem depois de ser convertido em RS-232 para a porta série do PC através do conversor indicado (figura 63).

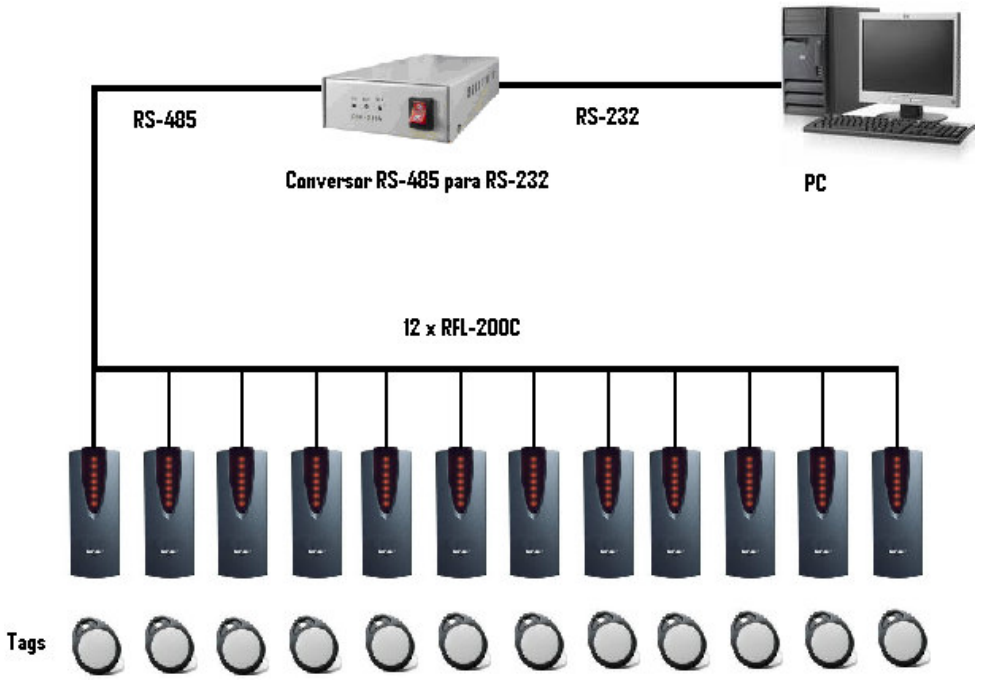


Figura 63 Esquema da Quarta Opção (Sistema Adoptado)

O preço final é de 140 € + IVA por cada um dos 12 dispositivos a ser instalados, adicionando o preço do conversor (54 € + IVA). A acumulação dos dispositivos perfaz então 2080 €.

Figura 64 RFL-200C

As potencialidades do RFL-200C são:

- Reconhecimento de RFID com codificação PSK de 128 bits a 125 khz;

- Comunicação em rede via RS-485 (max 255 canais);

- 512 Utilizadores / 256 eventos;

- *Upgrade* de *firmware* via *software*

- Totalmente selado e à prova de água

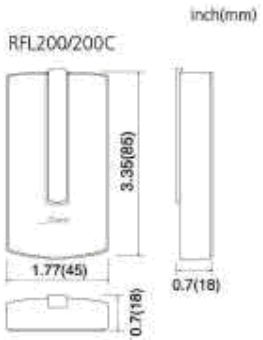


Figura 65 Dimensões do RFL-200C

Para todas as opções apresentadas verificou-se que independentemente dos protocolos a que comunicassem existia sempre a necessidade de existência de conversão do sinal em RS-232. Na figura 66 apresenta-se o *hardware* em causa.

Figura 66 CNP-200a

- Sinal RS-422 convertido para RS-232;

- Comunicação *Multi-Drop* ou Ponto a Ponto;

- Protecção Alimentação Interna;

Para a instalação dos equipamentos a empresa Telemax disponibilizou-se de imediato para ter em regime de permanência, um técnico que acompanhasse a instalação num máximo de 8 horas.

A implementação concretiza-se com a instalação de equipamentos de validação em 12 salas (numeradas de 1 a 12) da Academia conforme a figura 67 documenta. A instalação da cablagem processa-se mediante o tipo de equipamento escolhido, sendo que neste caso em particular a instalação era bastante simples pois a partir do PC dedicado ao sistema bastava derivar a cablagem necessária à recepção dos sinais por parte dos 12 leitores.

Cada um dos leitores RFL-200c escolhidos funciona como uma unidade independente e estes serão ligados todos em série pelo protocolo RS-485, o que minimiza em grande escala a cablagem utilizada na instalação. Não necessita por isso de conversores para transformação de sinais permitindo que até 16 unidades estes possam ser ligados em rede sem qualquer tipo de adaptação tecnológica.

Todos estes leitores ligam ao PC que é a base de todo o sistema elaborado. Recolhe as informações dadas pela rede de leitores, e regista-a para identificação e posterior tratamento. Esta unidade é um simples PC que não necessita ter grandes capacidades de processamento ou armazenamento, sendo que somente é necessário que tenha Visual Basic e Access, que são os constituintes do *software* de base do sistema.

Na figura 67 podemos ver esquematizada a planta das instalações com a colocação de todos os componentes explicitados. O PC tem de permanecer ligado para o bom funcionamento do sistema.

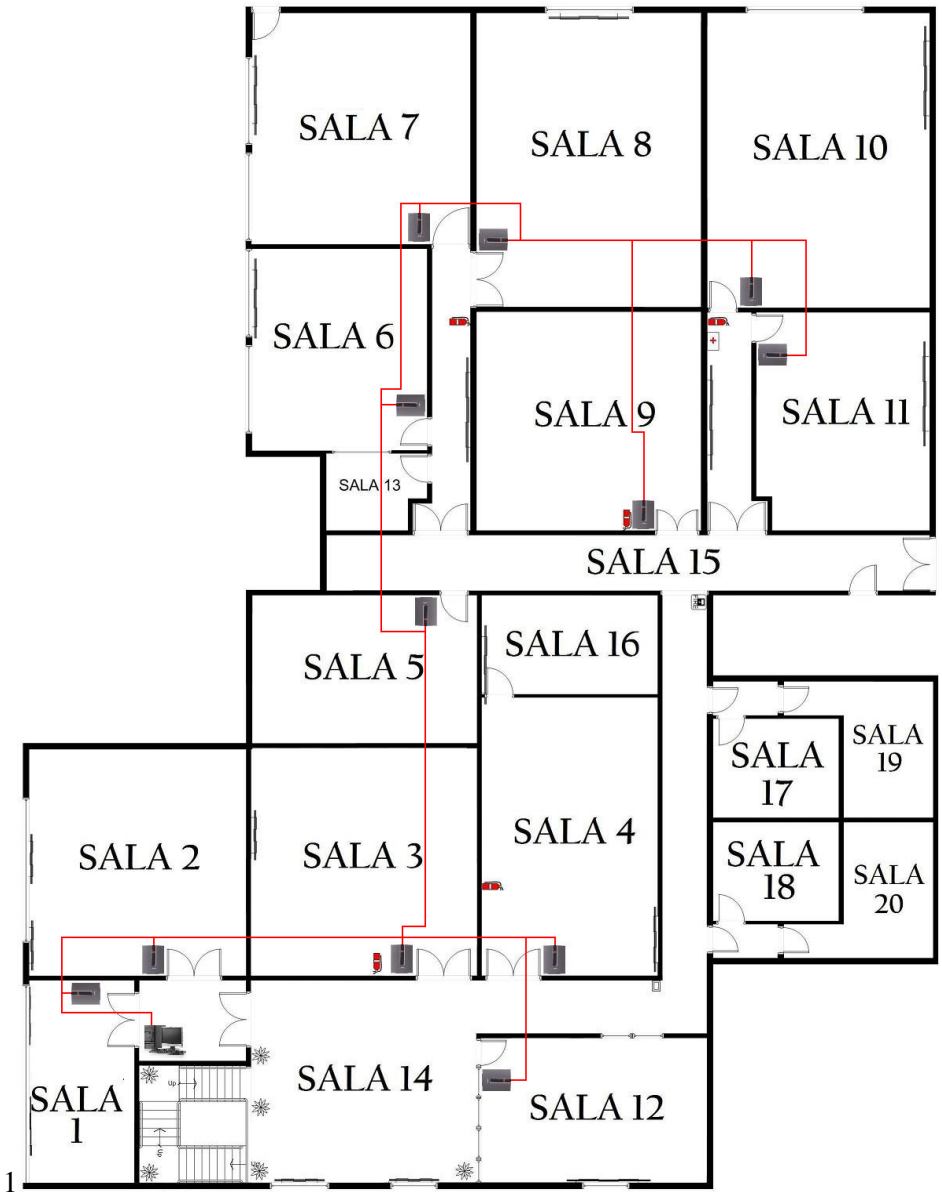


Figura 67 Planta Instalação Sistema

5.2.3.5 TAGS

Para que os utilizadores possam fazer a validação para além dos leitores tem de existir também as etiquetas individuais/pessoais. Para a escolha das *tags* foram apresentadas duas

soluções da IDTECK (figura 68). A primeira consistia num cartão (*smartcard*) que funcionava como uma qualquer etiqueta passiva, havendo ainda a opção de possuir *chip* para registo de informação adicional, como por exemplo dados pessoais ou outras informações úteis à empresa. O custo desta solução era de 0,10 € por cartão.

A segunda opção era a utilização de uma *tag* em tudo equivalente ao cartão, em termos de funcionamento, mas sob a forma de porta-chaves. Esta solução foi mais consensual dada a sua mais interessante portabilidade, apesar do preço ser de 0,13 €.

Sendo assim o custo total relativo à aquisição das 200 *tags* necessárias, seria de 26 €.

Figura 68 Tags IDTECK IDC 80 / LXK50

As características destas etiquetas são:

- Modulação PSK, 128 bits

- Cartão com formato e espessura ISO (IDC80)

- Editáveis e Possibilidade de impressão sobre o cartão (duas faces);

- Tag de transporte em porta-chaves (IDK50)

- Possibilidade de programação de cartões através de programador PRG1000

- Cartão tipo Crédito com espessura ISO;

- 13,56 MHz, compatível com ISO14443, tipo A;

- Cartão tipo Passivo, sem alimentação interna;

- 1 kB EEPROM;

- Função de escrita e gravação (com leitores / Gravadores tipo (RW) e programador (RG2000 SmartCard);

- Retenção de dados por um período nunca inferior a 10 anos;

- 100 000 Gravações por cartão;

5.2.3.6 COMPUTADOR

No que diz respeito ao PC utilizado no sistema este já existia nas instalações sendo uma máquina de relativo baixo custo, pois a natureza do projecto também não implicava elevadas performances de cálculo. Apresentam-se então as características do mesmo:

- Pentium 4 a 3,0 GHz

- 512 Mb de RAM

- 40 Gb de Disco Rigido

- Sistema Operativo: Windows XP SP3

5.2.4 SOFTWARE

Foi proposto pela Telemax a aquisição de um *software* de controlo de acessos. O custo deste era de 1000 Euros com formação incluída e dava pelo nome de AEON – Time & Attendance. No entanto a ideia sempre foi a de aproveitar o SDK (programa de comunicação do equipamento) que era fornecido gratuitamente (para edição) e tratá-lo com uma base de dados dos activos em Microsoft Access com chamadas de Microsoft Visual Basic. Na figura 69 apresentam-se uns *screenshots* do *software* da Telemax.

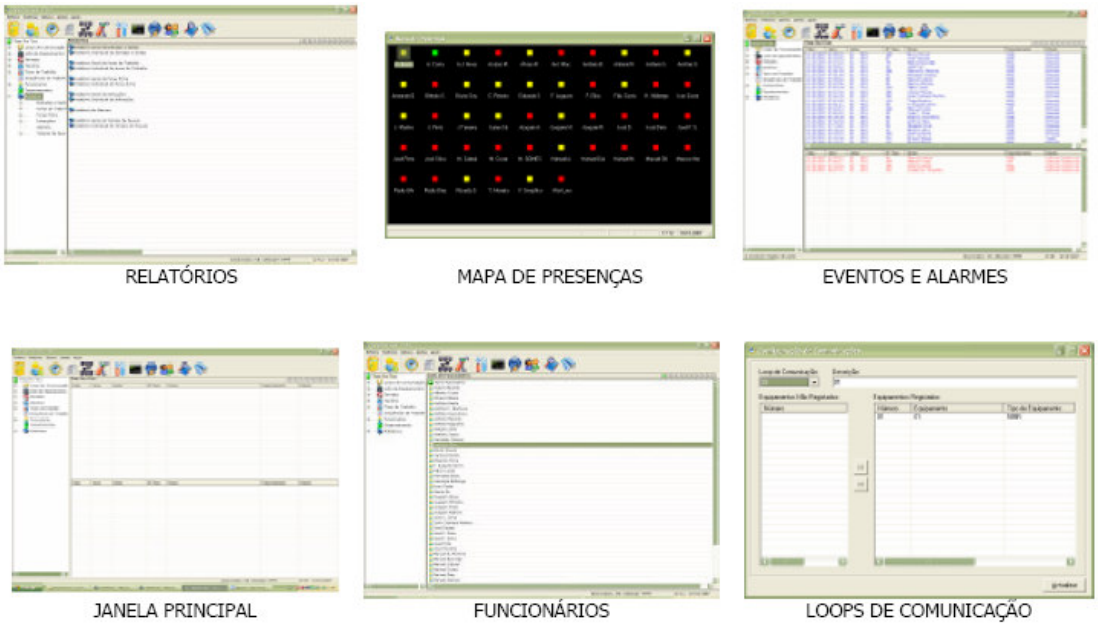


Figura 69 AEON – Time & Attendance

Sendo assim delinearam-se objectivos uns que foram posteriormente conseguidos e outros que ficam para uma futura abordagem. As características principais do software desenvolvido tinham então por objectivo:

Características Gerais (Operação)

- Microsoft Windows XP (Home, Pro), Vista®

- Exportação de dados por Excel ou Texto

Definições de Segurança e Acesso

- Definição de utilizadores

- Definição de níveis de acesso (Futura Implementação)

- Restrições e inibições de acesso (Futura Implementação)

Evolução e Upgrades

- Integração com sistemas de Recursos Humanos (Futura Implementação)

- Criação de interfaces comunicacionais (utilizadores)

Características de Controlo

- Planeamento individual de horários (Futura Implementação)

- Criação de horários livre, fixo, flexível, por turnos, com isenção, inibição de controlo, estatutos próprios, turnos especiais (Futura Implementação)

- Criação de Tabelas de Horário Semanais a Bianuais (Futura Implementação)

- Emissão de justificações prévias e posteriores

- Edição completa de férias, folgas, folgas especiais, dias de descanso, dias sem trabalho

- Controlo de faltas com ½ dia

- Gestão de férias (Futura Implementação)

- Verificação em tempo real de trabalhadores

- Planeamento de escalas e turnos

- Contabilização de horas, pausas, faltas, folgas

Relatórios

- Registo de presenças e ausências

- Verificação de pausas e paragens para refeições

- Controlo de colaboradores

- Controlo de infracções – Atrasos e saídas antecipadas

- Falta de registos e justificações

- Infracções e dias de ausência

- Trabalho normal, extra, especial

- Controlo diário, semanal e mensal

- Emissão de relatório completo por utilizador

Controlo em Tempo Real

- Interface gráfica de controlo de presença e ausência de funcionários com actualização em tempo real

- Interface gráfico de controlo de faltas / falhas geral e por departamento

Tecnologias de Reconhecimento

- Reconhecimento RFID

Definições Comunicação

- Comunicação Série (RS-232 / RS-422 / RS-485)

A forma como o software foi desenvolvido decompôs-se em variadas fases, devido a adaptações e problemas conjuntos que se passam a citar.

5.2.4.1 PROCESSOS SISTEMA

A arquitectura tem como funcionamento numa primeira instância, e como não podia deixar de ser, a figura principal na pele do utilizador que se pode validar, por um método:

- Apresentação da Etiqueta RFID que detêm, pessoal e intransmissível;

Qualquer tentativa de validação, implique sucesso ou não, deve indicar na interface gráfica (computador), o estado da mesma para informação em tempo real.

Se a validação não tiver sucesso por não leitura da etiqueta, o utilizador tem de tentar até que se consiga validar.

- No caso de ter sucesso na validação, então a informação do mesmo é transmitida à base de dados para que se possa saber se este está devidamente identificado nesta. Se não estiver

identificado, então isso significa que o indivíduo não pode entrar neste sistema, ou então terá que solicitar um registo de acesso.

- Se estiver identificado, é então enviada a informação de validação do utilizador para o registo, que "escreve" a data e a hora no sistema, neste caso, mais propriamente na base de dados.

Caso o utilizador tente fazer involuntariamente – ou por dúvida se já se registou ou não, ou por aproximação inadvertida da etiqueta do leitor – um novo registo num espaço de tempo inferior a 1 minuto existe o retorno da situação de "Logon Duplo" e não efectua o registo.

O sistema permanece constantemente em *standby* (depois de configurado para comunicação). No que diz respeito às validações, caso o activo tenha registado uma entrada nas instalações – registada na Tabela da Base de Dados – o programa aguarda a sua saída. No caso de este ter validado já uma saída, então a programação aguardará uma consequente entrada.

No que diz respeito à Interface Gráfica que é a última etapa do sistema, esta transmite as *mensagens* de sucesso e de erro para o monitor anexo ao sistema. São colocadas mensagens no monitor do sistema (Interface Gráfica) que se resumem às expostas na tabela 16.

Validação com Sucesso	Registada a entrada do utilizador X às HH:MM
Saída com Sucesso	Registada a saída do utilizador X às HH:MM
Validação sem Sucesso	Utilizador Inexistente!
Logon Duplo	"Identificação do utilizador fica a negrito"

Tabela 16 Possíveis mensagens Interface Gráfica

5.2.4.2 CONSTRUÇÃO ROTINAS

A base para a projecção da programação neste projecto reside na construção de ciclos por linguagem orientada a eventos com camadas de aplicações. Comummente usada nos dias de hoje, esta prima pela facilidade de construção e pelo excelente resultado visual que proporciona tanto ao programador como ao utilizador da dita programação.

Observação: As únicas funcionalidades não representadas adiante são as de complementaridade de Access e Visual Basic, como por exemplo os retornos de formulários, etc.

Por isso mesmo o núcleo desta programação assenta sobre alguns programas para o desenvolvimento do *software*.

5.2.4.2.1 BASE DE DADOS (MICROSOFT ACCESS)

Em Access está definida a base de dados do sistema (T_UTILIZADORES), todos os activos que entram e saem das instalações têm de estar presentes na mesma (figura 70). Os campos de identificação de cada utilizador são o nome, o número interno na Academia (também designado Código de Utilizador e essencial para o tratamento na aplicação) e a turma ou cargo que desempenha nas instalações (figura 71).

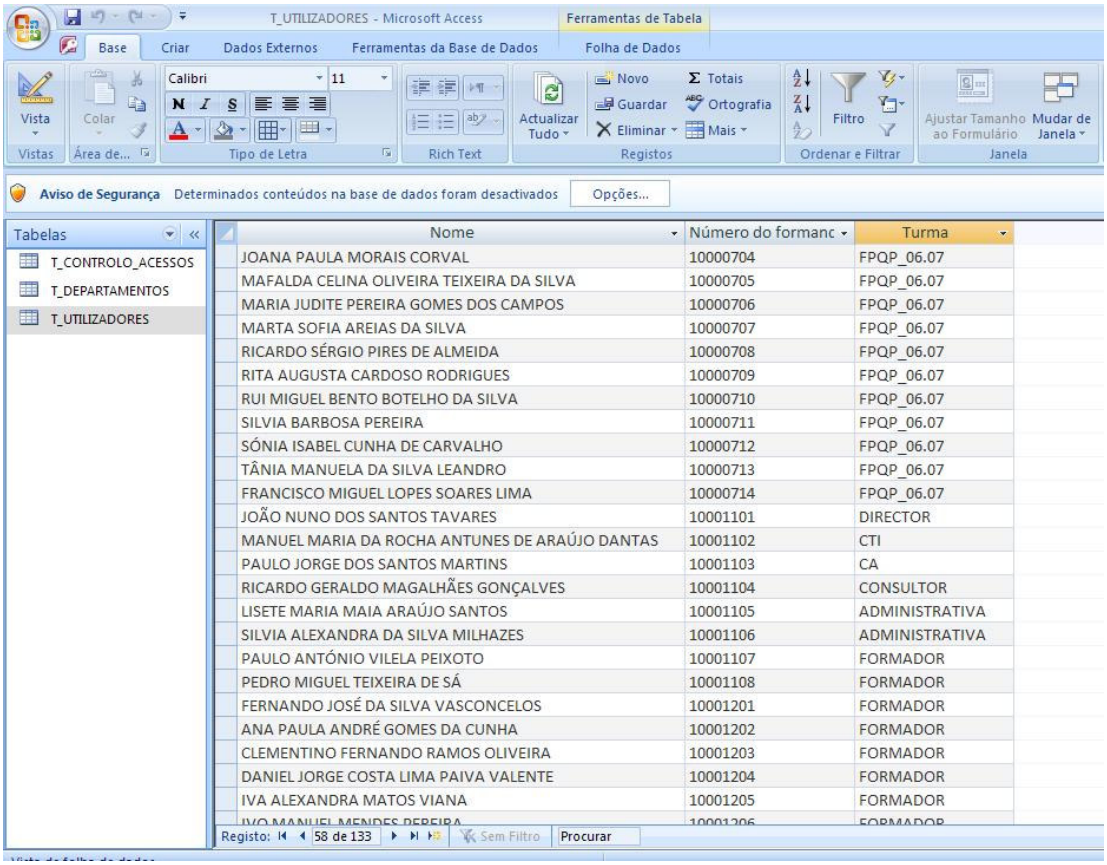


Figura 70 Base de Dados (T_UTILIZADORES)

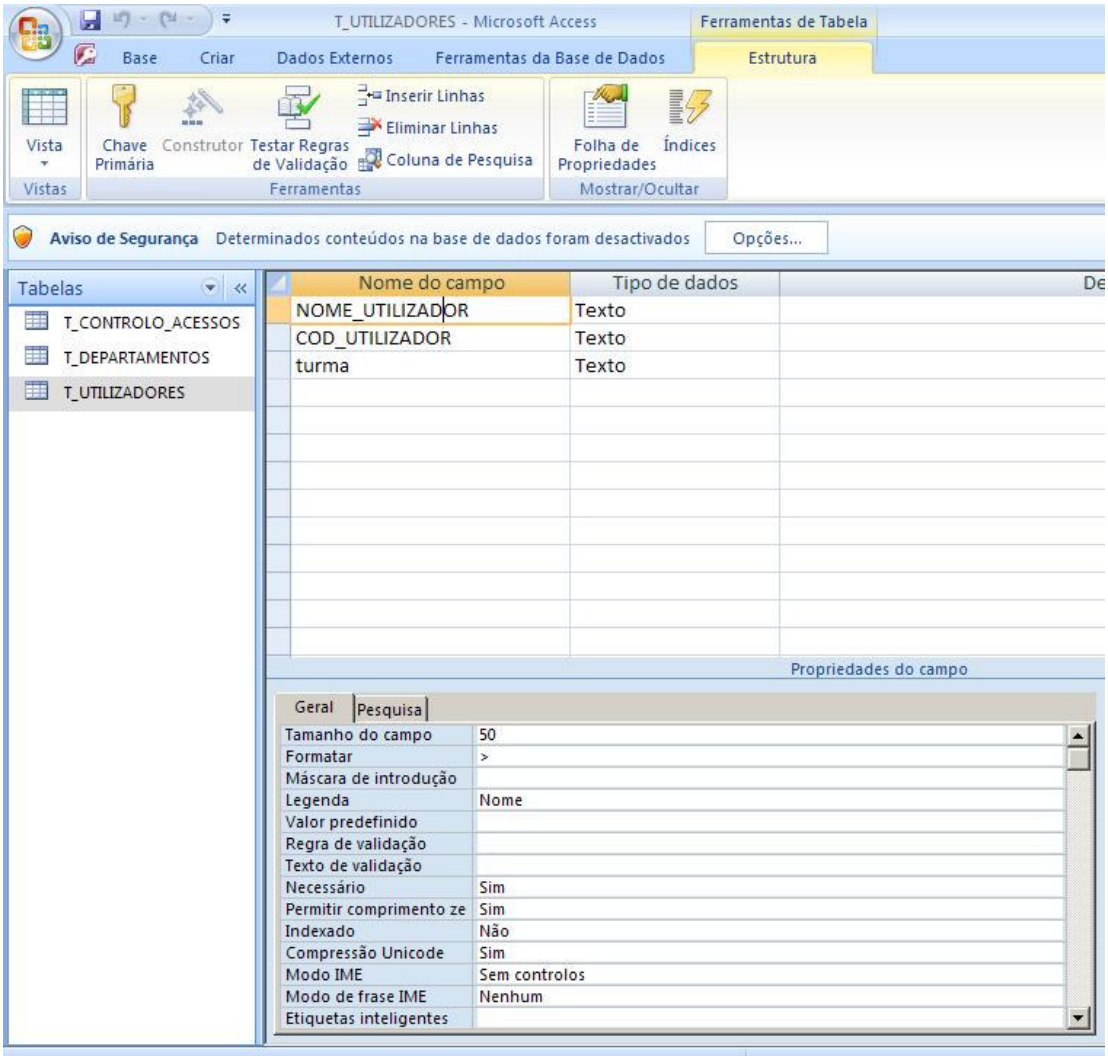


Figura 71 Campos Base de Dados (T_UTILIZADORES)

Existe ainda a tabela T_CONTROLOS_ACESSOS (figura 72) que trata o registo de entradas e saídas que pode ser "a posteriori" exportado com toda a facilidade para uma comum folha de Excel. Esta tabela é essencial por conter toda a informação a ser tratada de entradas e saídas dos elementos e facilita a visualização do tempo que um activo esteve na empresa num determinado dia. Os campos pelo qual é composta são o Código de Utilizador (Número Interno), a data e hora de *login* e a data e hora de *logout* que estão apresentados na figura 73.

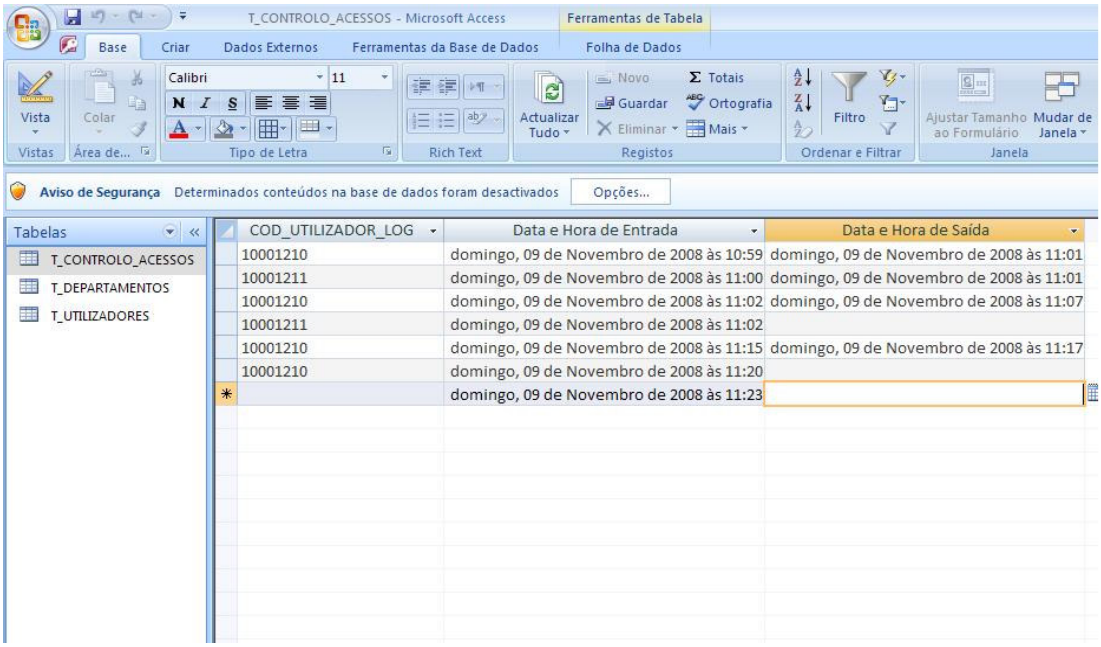


Figura 72 Registo Base de Dados (T_CONTROLO_ACESSOS)

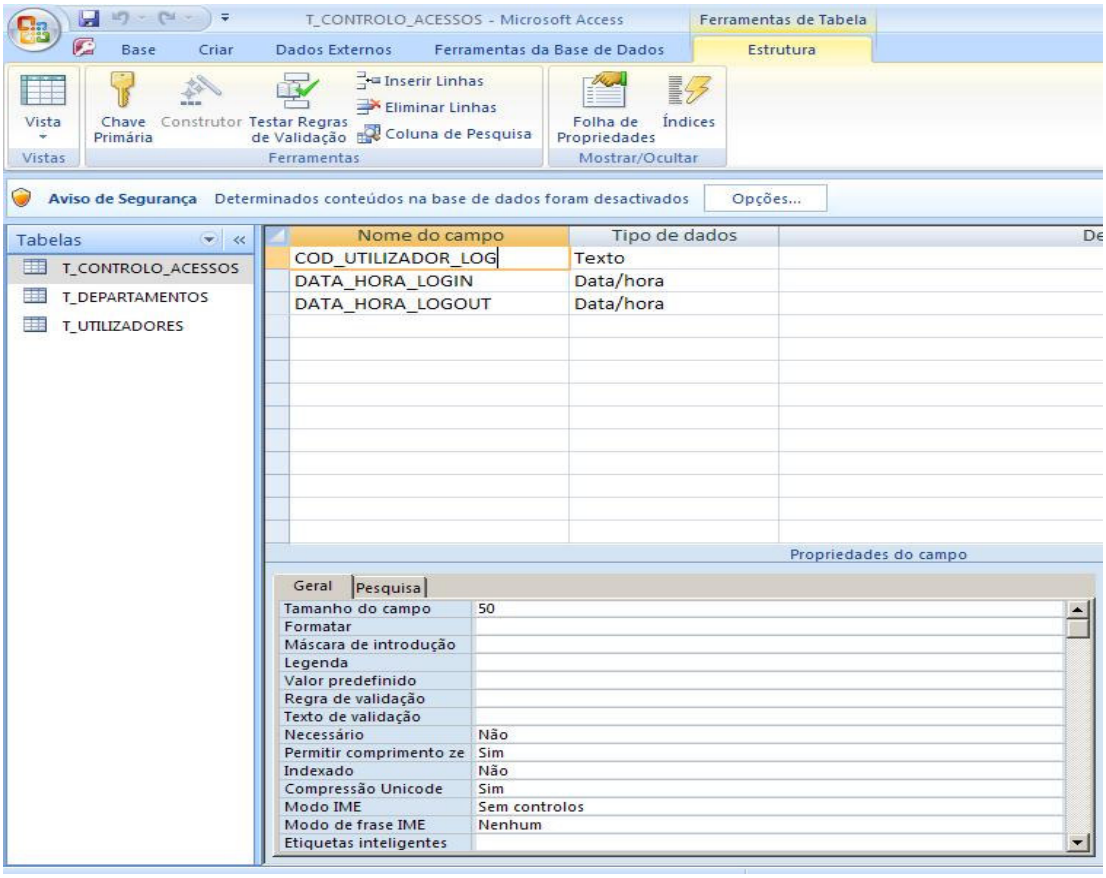


Figura 73 Campos Tabela Registo na Base de Dados (T_CONTROLO_ACESSOS)

Na exportação e consequente tratamento dos dados pode-se ainda fazer a selecção de informação através dos vários departamentos da Academia. A tabela T_DEPARTAMENTOS (figura 74) trata essa questão. Os seus campos constituintes são os representados na figura 75.

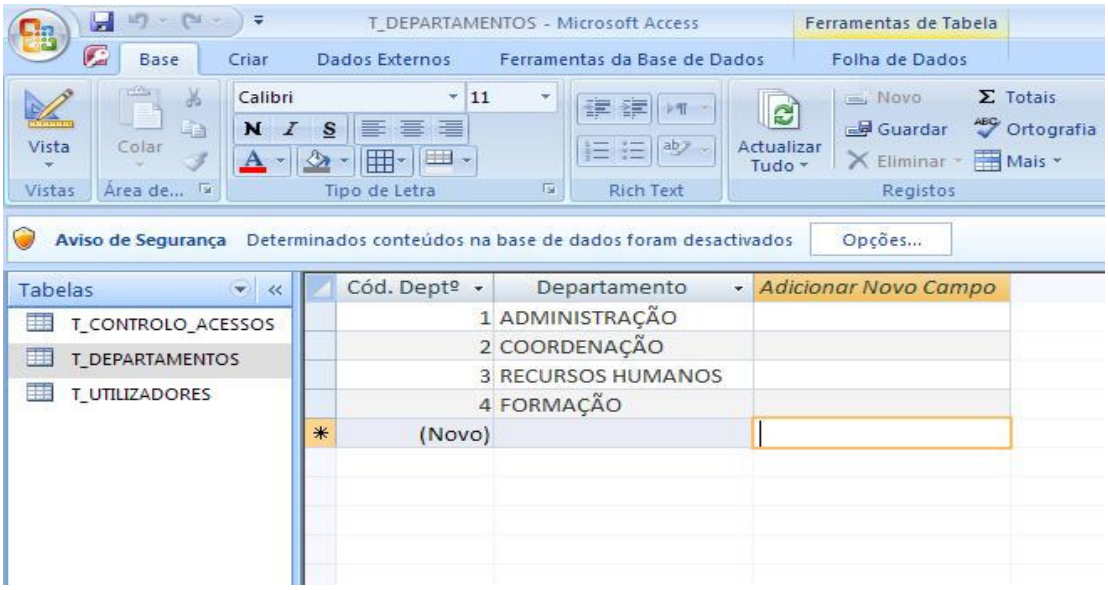


Figura 74 Tabela de Divisão Departamentos (T_DEPARTAMENTOS)

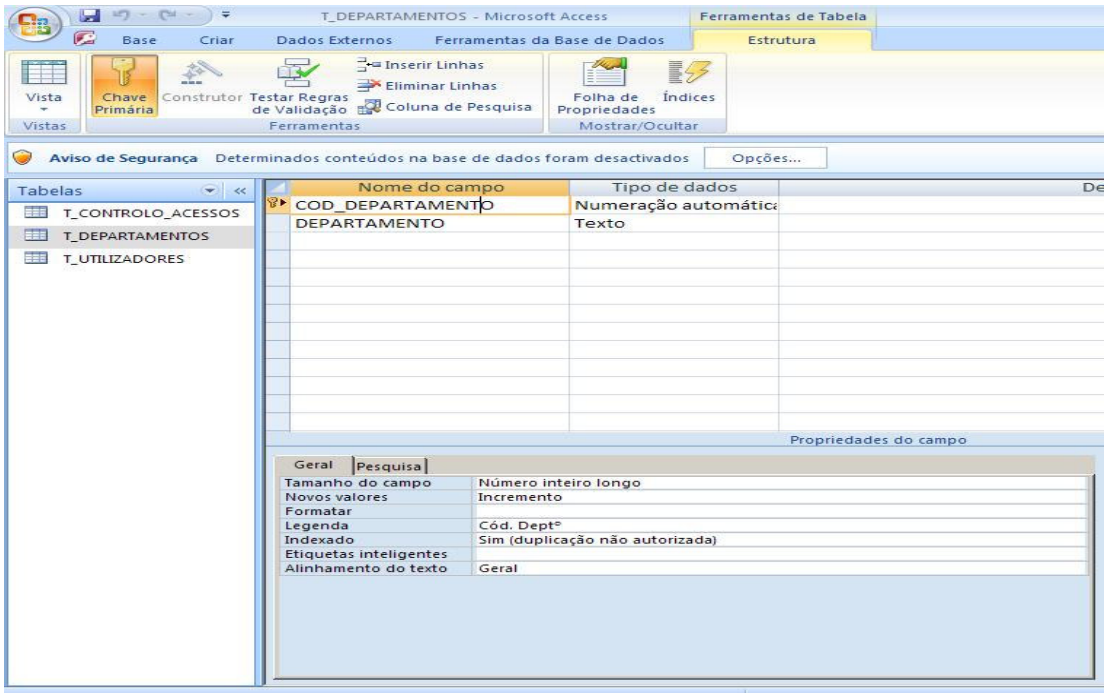


Figura 75 Campos Tabela Divisão Departamentos (T_DEPARTAMENTOS)

5.2.4.2.2INTERFACE GRÁFICA (MICROSOFT VISUAL BASIC)

O sistema tem de funcionar com as partes. Para que seja possível a interligação entre a base de dados e o *hardware* usou-se Visual Basic (VB). O resumo apresenta-se no fluxograma (figura 76).

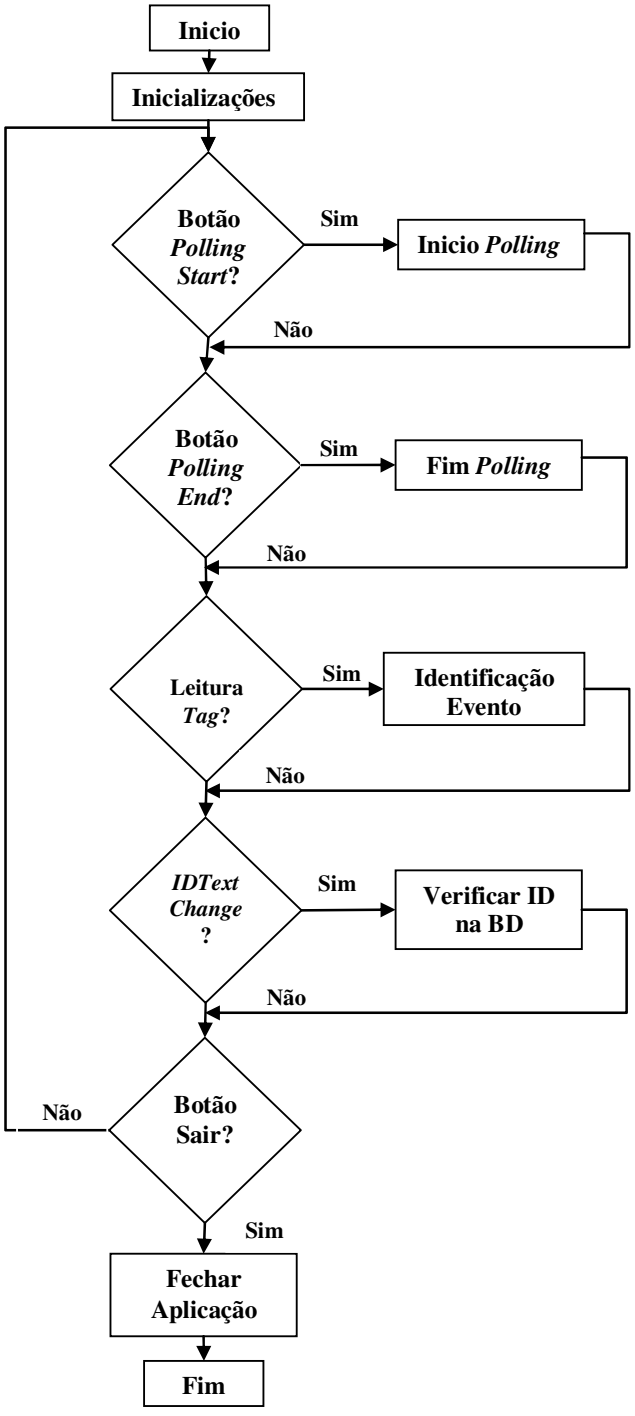


Figura 76 Fluxograma Interface Hardware (Visual Basic)

Tal como dito anteriormente, a linguagem de programação deste software é extremamente acessível, igual ao Access, e por isso as grandes dificuldades somente residiram na adaptação a algumas particularidades/exigências que este possui.

A partir do fluxograma da figura 76 poderemos subdividir as tarefas que este concretiza.

- Iniciações

O objectivo é fazer a definição dos parâmetros de comunicação.

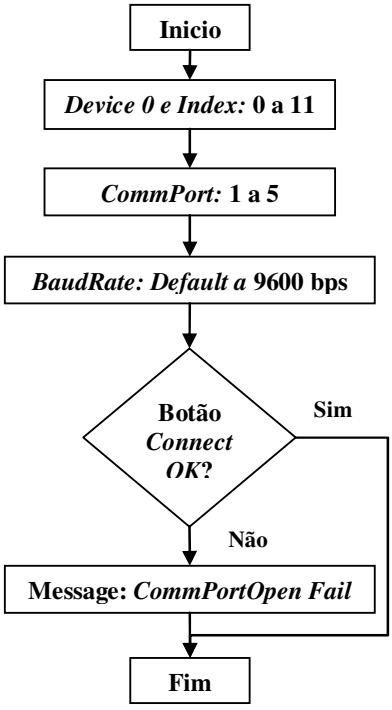


Figura 77 Fluxograma das Inicializações

Logo no início encontram-se as definições de funções que nos permitem fazer a chamada do ficheiro do próprio *hardware* para que se proceda à abertura da porta de comunicação (COM). Selecciona-se o dispositivo (neste caso o Device 0 que vai ser a plataforma de comunicação de todos os leitores), juntamente com o ID de todos os leitores. Pode-se definir, um número de porta COM que se queira por defeito, assim como de *BaudRate* (velocidade de transferência dos dados da porta em questão). A figura 77 ilustra o fluxo de informação e a 78 ilustra o esquema completo de definições.

Por defeito definiu-se a COM 5, device índex 0 e baud rate de 9600 b/s.

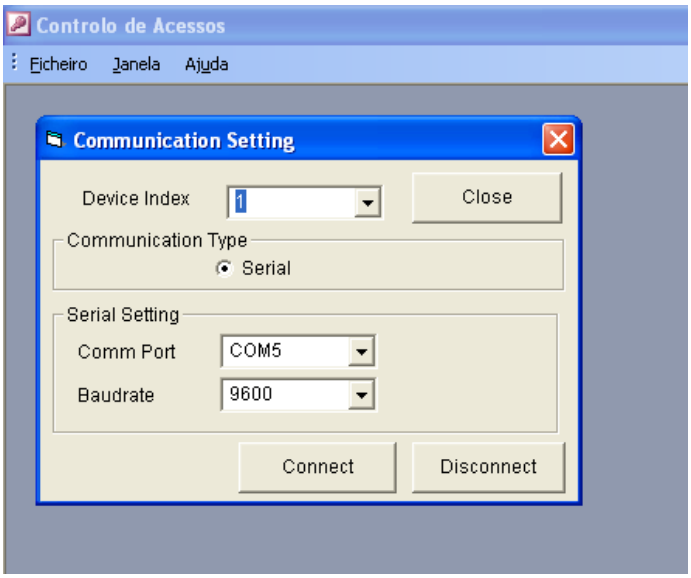


Figura 78 Definição Comunicação

- Pollings

Centra-se na definição das variáveis necessárias ao longo do programa, como por exemplo a chamada do *Polling Start* que não é mais do que a obrigatória troca de sinais que tem de existir entre o hardware e o software para que possa haver envio correcto de dados, e sinalização de prontidão do primeiro. Claro está, que pela lógica da função seguinte um *Polling End* será para fazer o inverso, ou seja, a paragem de troca de informações.

Se não for possível executar o *Polling Start* o sistema nunca entrará em acção. Após as definições de comunicação estarem realizadas é obrigatório que este aconteça.

A todo o momento pode-se executar um *Polling End* que interrompe toda e qualquer troca de sinais repondo todas as definições até então, aos seus valores *default.*

Nas figuras 79 e 80 estão representados os fluidos de execuções dos *Pollings*.

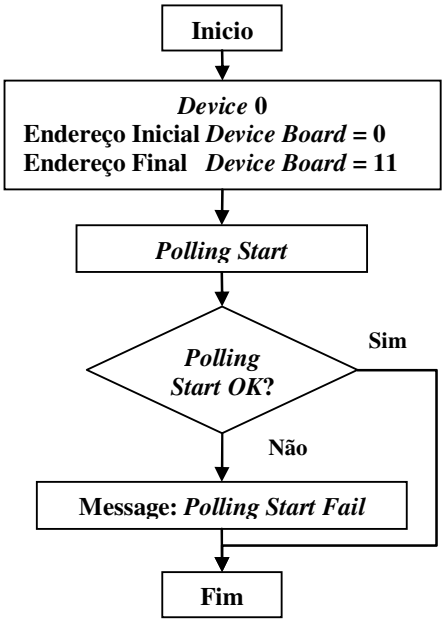


Figura 79 Fluxograma *Polling Start*

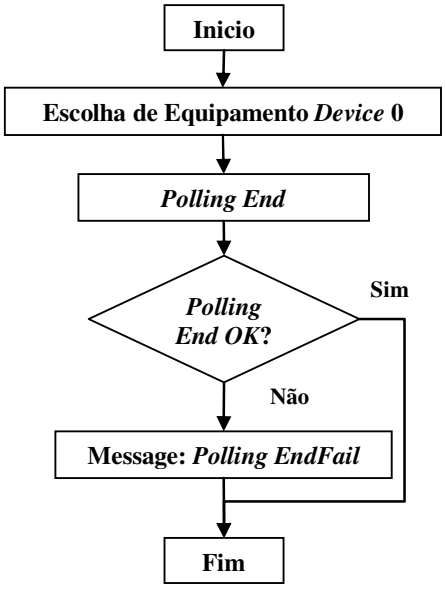


Figura 80 Fluxograma *Polling End*

Os dois fluxogramas expressam que em primeira instância é necessário seleccionarmos o equipamento a ser configurado e depois as verificações de sucesso ou falha da execução da

respectiva função. Na figura 81 está representada a janela que permite executar na aplicação os *Pollings*.

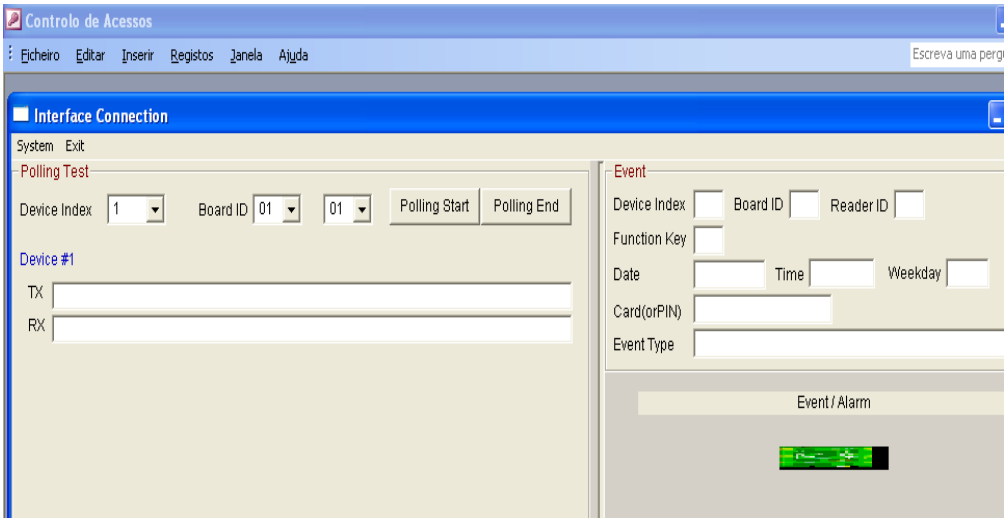


Figura 81 Janela de activação dos sinais *Polling*

Esta é a janela do programa identificada por *Interface Connection* onde se podem visualizar do lado esquerdo as definições feitas até então na comunicação, os botões de *Polling,* e mais abaixo os campos que exibem os códigos máquina em tempo real de troca de sinais TX e RX (diferenciados por cores) entre aplicação e o equipamento.

Do lado direito da mesma figura encontram-se os campos que sempre que se dá um registo vão assinalar as informações relativas a esse mesmo registo. É um controlo interno visual que o utilizador não deverá ver, mas que o programador tem como salvaguarda caso as mensagens da Interface Gráfica falhem. São apresentados dados relativos a qual dos 12 equipamentos validou uma entrada, a identificação da sua placa e do número do leitor, a data, hora e dia da semana e por último o tipo de cartão utilizado (sempre o mesmo) e o tipo de evento (entrada ou saída).

- Identificação Evento

Nesta parte de VB está ainda feita a compatibilidade e armazenamento de informações que vão ser tratadas posteriormente nomeadamernte qual dos leitores efectuou a leitura, a data, hora e estado da passagem da etiqueta pelo leitor. Quando recepcionadas estas informações dá-se a modificação de uma variável denominada *IDText* que contem todos estes dados,

que são passados a uma outra variável chamada *IDCard* (necessária para o tratamento da informação em VBA). É disparado um evento chamado de *IDTextChange* que vai ser utilizado depois para a passagem da informação.

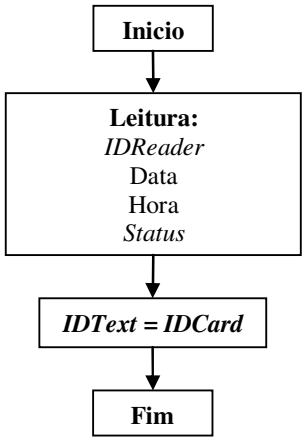


Figura 82 Fluxograma da Identificação completa do Evento

Antes do tratamento das informações ser feito em VBA, são actualizados alguns campos em VB que facilitam depois a manipulação dos dados. Faz-se uma ligação ao MS Access de forma a activar a plataforma de VBA, sendo que antes já haviam sido actualizados os campos USR e *Reader*, necessários a esta passagem de informação. Será a partir destes que se faz a ligação de VB para VBA. O fluxograma da figura 83 relata isso mesmo.

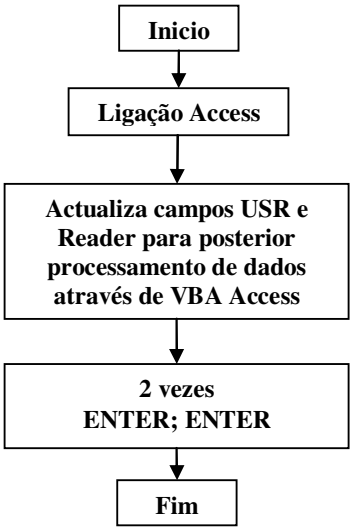


Figura 83 Fluxograma da passagem da informação do Hardware para VBA

Por último, para que o sistema fique pronto a tratar a validação são dadas duas ordens de "Enter", para que este, mesmo sem rato, possa sair do campo de representação do Código de Utilizador (número 1 na figura 84), e de seguida dar entrada desse mesmo número no sistema (número 2 na figura 84) para que possa ser analisada a informação.

Figura 84 Janela que recebe o comando "Enter" duas vezes

Desta forma o sistema fica pronto para fazer o tratamento de toda a informação recolhida pelo *hardware*. Caso se queira sair desta componente de configurações (em VB) o procedimento é o apresentado no fluxograma da figura 85.

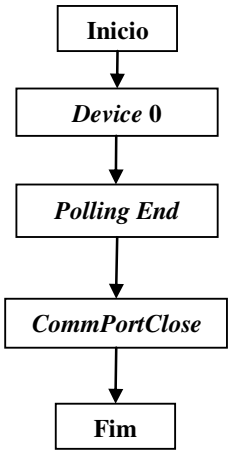


Figura 85 Fluxograma de saída da Interface Hardware

5.2.4.2.3 INTERFACE TRATAMENTO DADOS (MICROSOFT VISUAL BASIC APPLICATIONS)

Após todas as configurações o sistema fica pronto para a validação. Sendo assim quando este se encontra preparado ou em *standby* a interface gráfica (PC) apresenta a caixa da figura 86.

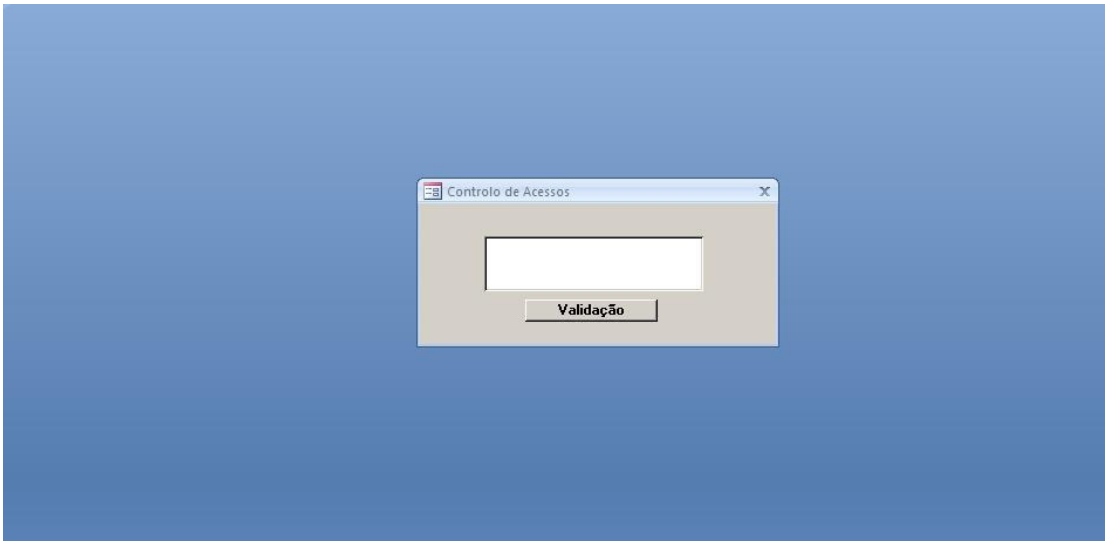


Figura 86 Interface Identificação do Utilizador

Depois de toda a componente de compatibilização dos sinais de *hardware* ter sido tratada em Visual Basic, o tratamento dessas variáveis com informação é feita em Visual Basic Applications. Esta linguagem é um pouco mais acessível e mais fácil de programar.

Nesta parte do desenvolvimento foi criada uma função *DoThings* que é a principal do programa. Testa as condições necessárias ao processo de login, onde se inclui na sequência a contemplação de "utilizador inexistente" e a forma de aparecimento das mensagens após actualização das entradas/saídas, com especial relevância para o último registo efectuado, assim como o Logon Duplo. Após o último "Enter" dado na versão da *Interface Hardware*, o VBA entra em acção activando a *DoThings*. Se se carregar no botão Fechar da Janela da *Interface* é dada saida do sistema.

Estas execuções estão representadas na figura 87.

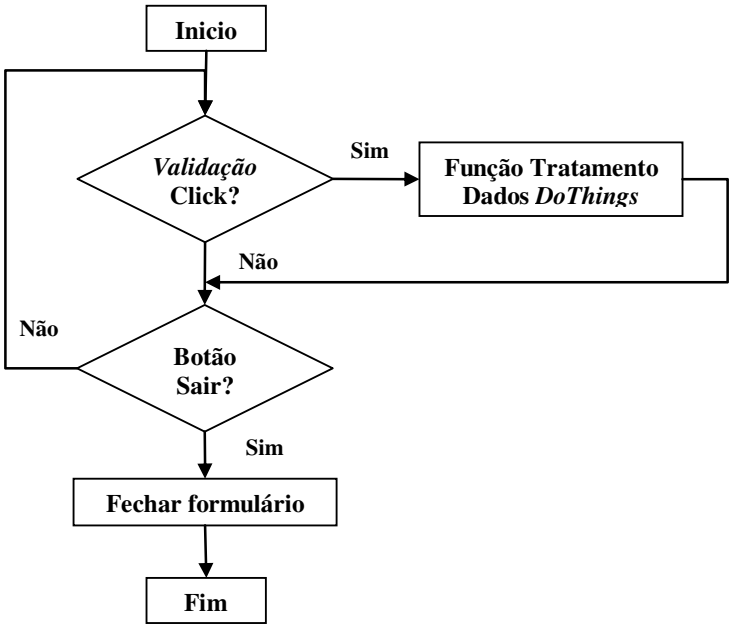


Figura 87 Fluxograma de Recepção e chamada da Função *DoThings*

- Função Tratamento Dados *DoThings*

O que foi feito até agora foi:

Sempre que um activo aproxima o cartão do leitor, esta proximidade devolve pelo equipamento para a aplicação um código interno que identifica a presença ou não de um membro do sistema.

O que a função *DoThings* faz (figura 88), é que pela consulta à Base de Dados (mais propriamente à tabela T_UTILIZADORES), por comparação dá o resultado de inscrição desse mesmo membro ou não nos arquivos.

Caso não haja registo do número interno (Código Utilizador) na tabela T_UTILIZADORES de uma etiqueta apresentada, então é devolvida a mensagem de "Utilizador Inexistente" e não é feito qualquer registo de entrada ou saída na tabela T_CONTROLO_ACESSOS (figura 89).

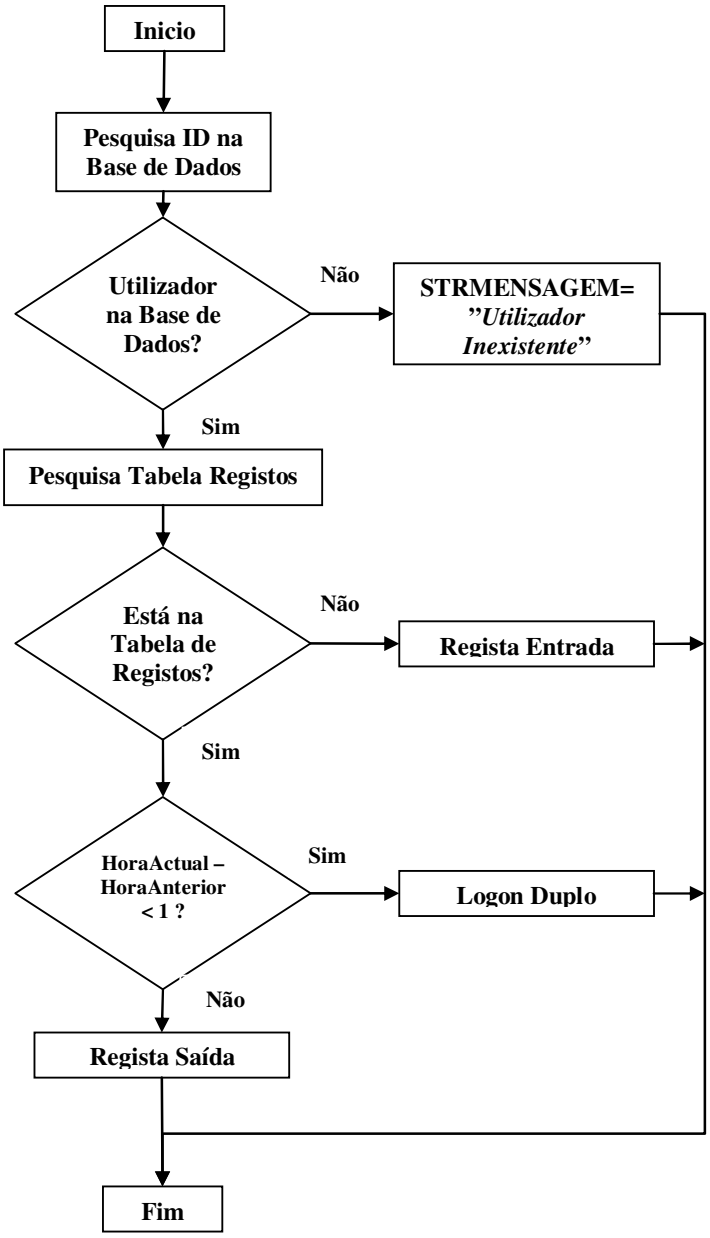


Figura 88 Fluxograma da Função *DoThings* (Tratamento dos Dados)

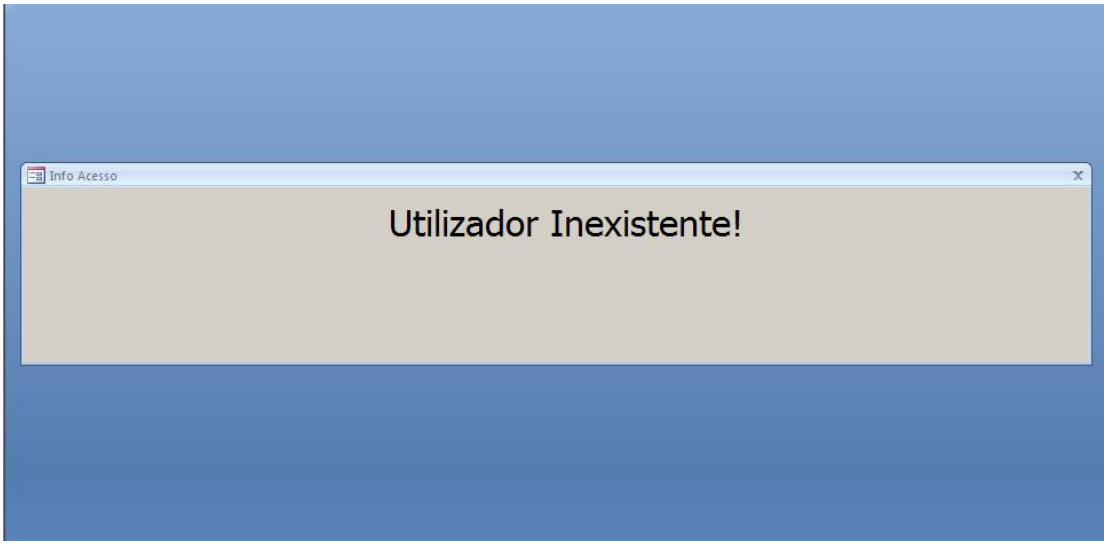


Figura 89 Mensagem de Utilizador Inexistente

A tabela T_CONTROLO_ACESSOS, regista nas validações o nome do utilizador e a sua hora e data completas de entradas e saídas. Se existir, é consultada a tabela T_CONTROLO_ACESSOS verificando-se se essa mesma pessoa já se encontrava validada. Se ainda não estiver nas instalações (registo não presente na tabela de registos T_CONTROLO_ACESSOS) então é feita a respectiva validação e apresentada a imagem da figura 90.

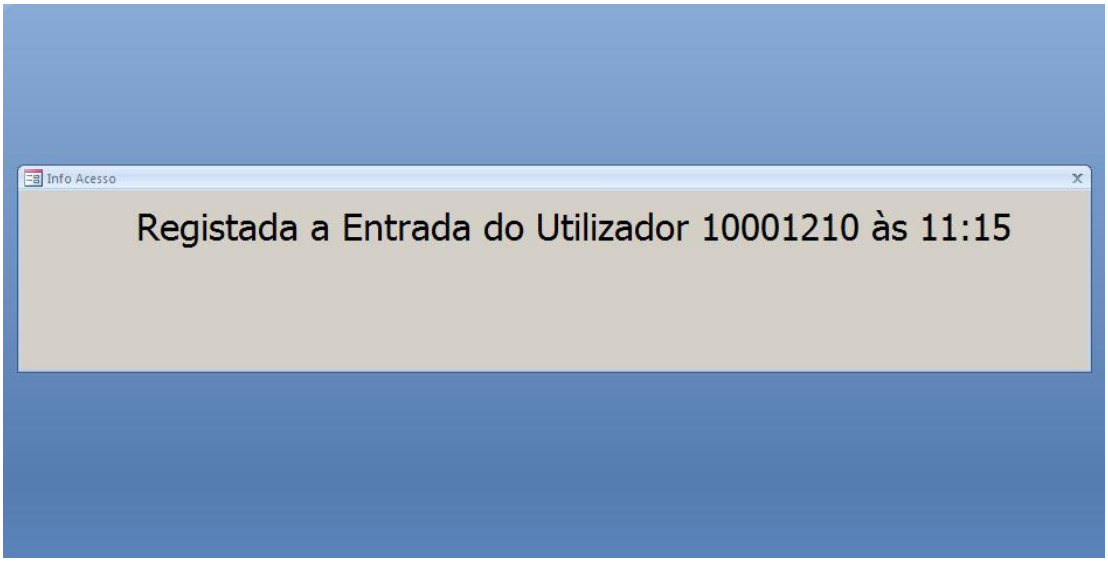


Figura 90 Entrada Utilizador

- Logon Duplo

Como já foi referenciado na tabela 16, nas possibilidades de aparecimento de mensagens, existe uma funcionalidade contemplada na programação deste sistema que se define como um mecanismo do tipo *fail-safe*, e que na realidade evita possíveis erros humanos na respectiva validação (figura 88 e 91).

É realizada uma comparação entre a data e hora actuais com a data e hora da tabela T_CONTROLO_ACESSOS e se o resultado for inferior a 1, é executada a situação de Logon Duplo. Ocorrendo esta situação o utilizador não é validado até que passe este intervalo de tempo.

A ocorrência desta situação deve-se à involuntariedade de por vezes as pessoas passarem a etiqueta sem intenção, ou porque não têm certeza se já o fizeram ou porque não tiveram alguma confirmação visual ou sonora da respectiva validação. Pode ainda ocorrer a questão de que se a pessoa deixar ficar a *tag* durante muito tempo em frente ao leitor, movendo-a poderia registar múltiplas entradas/saídas. Este mecanismo serve precisamente para salvaguardar situações de distracção, ou até mesmo de imprecisão de leitura RFID.

Figura 91 Logon Duplo

Quando ocorre um Logon Duplo a Interface Gráfica representa o Código de Utilizador a negro (seleccionado) não representando qualquer mensagem de validação.

Caso não ocorra Logon Duplo, significa que o utilizador já tinha sido validado num espaço superior a um minuto e então é dada a sua saída do sistema, sendo apresentada a mensagem da figura 92.

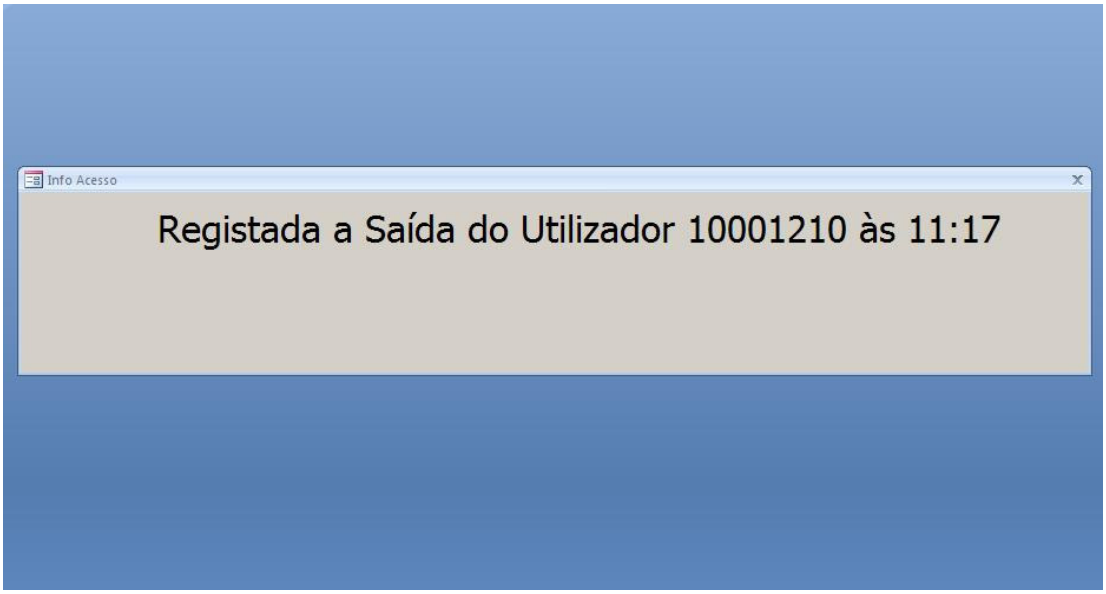


Figura 92 Saida Utilizador

Existem algumas outras particularidades do código para evitar possíveis situações complicadas:

- Foi criada uma rotina específica para que os dados comparados com a Base de Dados não tivessem de ser *Case Sensitive*. Desta forma escrever "Manuel Teixeira" ou "MaNuEl TeIXeIrA" é exactamente igual para o resultado da comparação.

- Para que se pudesse ter conhecimento das "*hardware faults*", foi criado um ciclo de instruções que permite reportar desta forma esses erros para melhor identificação, principalmente no desenvolvimento do *software*, esta rotina acabou por se mostrar de extrema importância (programada em VB).

- Caso o *hardware* se disconecte por uma razão qualquer (problema ocorrido durante os testes), foi também criado um ciclo para que seja de forma automática feito um *Polling End*.

- Numa perspectiva de implementação futura existe ainda a possibilidade de ligação de vários outros equipamentos a este, e em consequência, de manipulação de abertura ou fecho de diversos trincos de portas que se queira.

Quanto à linguagem a maior vantagem é sem dúvida, encontrada na fácil programação e nas rotinas extremamente semelhantes entre funções.

As desvantagens, que acabaram por se reflectir numa duração excessiva desta componente, residem basicamente, na ignorância de conhecimento de algumas obrigações de processo.

O desenvolvimento de toda a componente de *software* foi a que se revelou mais prolongada, devido ao desconhecimento de utilização do mesmo, e por ter sido por diversas vezes submetido a múltiplas fases de testes, na maior parte dos casos infrutíferas.

Foram salvaguardadas algumas posições importantes que permitem que o sistema funcione com um mínimo de falhas possível, talvez fosse também esta uma das causas para o lento desenrolar do projecto em algumas alturas.

6. CONCLUSÃO

A área de RFID é uma área que envolve recursos humanos na pesquisa, desenvolvimento e projecto de mais e melhores sistemas. Por ser uma tecnologia tão apetecida, o mercado é um constante "cliente" de novos desafios [37]. Como foi possível verificar ao longo da tese, a tecnologia RFID baseia-se em princípios de funcionamento básicos, com tecnologias simples mas de extrema utilidade e funcionalidade. Impõe-se a diminuição do tamanho e do preço do *tag,* mas exige-se o aumento de capacidade e a melhoria do alcance. A agilização dos procedimentos e o incremento no processamento dos dados permitem uma melhor visibilidade dos produtos. Isso garante um diagnóstico exacto, eliminando riscos de falha na previsibilidade e erros nos negócios, ou seja, maior lucro, menor perda de tempo e maior proveniência.

A tecnologia de Identificação por Radiofrequência não é somente uma questão tecnológica, mas sim também uma questão de padronização mundial, e o reconhecimento por todos os mercados comuns. A grande focagem nos custos descura muitas vezes questões como a qualidade da implementação dando origem à negligência de outros custos mais importantes na implementação deste tipo de tecnologias que passam pela análise dos processos e dos benefícios [37]. Na hora de implementar um sistema destes é imprescindível fazer uma análise do sistema, partindo das necessidades do negócio. Em jeito de resumo final,

verificou-se ao longo deste estudo que existem muitos sistemas RFID a funcionar, com variadíssimos modos de funcionamento e princípios de comunicação. Apesar desta grande variedade, os sistemas podem ser qualificados, grande parte das vezes, pelo modo de funcionamento dos *tags* usados. A generalização do uso dos *tags* passivos (por ter bom desempenho a baixo custos), levam a uma crescente aposta no seu desenvolvimento.

A nível da implementação espera-se que o apresentado nesta tese possa ter sido útil em duas frentes: no sentido de mostrar os conceitos básicos de controlo de acesso em aplicações; e no sentido de promover informação prática sobre um engenho de controlo de acesso que pode ser integrado por aplicações com um mínimo de esforço.

Existem várias possibilidades de melhoria do sistema e em alguns casos, não se detalharam alguns aspectos por serem mais simples e/ou bem entendidos (conceitos básicos técnicos, por exemplo). Em outros, por apresentarem oportunidades de pesquisas inteiras por si mesmo, sendo o tempo insuficiente para exploração (comunicação via TCP, por exemplo).

Dessa forma, entre os vários trabalhos futuros que podem ser vislumbrados, estão:

- Melhor tratamento da camada de dados, tornando-a mais flexível e extensível;
- Mais estações de validação para entrada individual de salas ainda não contempladas;
- Construção de um *software* mais "apetecível" para o utilizador comum;
- Construção de interfaces e métodos de configuração padronizados com outros *softwares* já existentes no mercado;
- Explorar mais opções passíveis de serem implementadas para melhor tratamento dos dados ou aquisição de novos elementos;
- Pesquisar mais a fundo e estender melhor os elementos não autorizados à programação do sistema, sendo que mesmo assim este encontra-se protegido por natureza como explicado atrás.

Anexo A. Principais Fabricantes de RFID [2]

Fabricante	Produtos	Fonte
Applied Wireless ID	Antenas, tags e readers	http://www.awid.com
Alien Technology	Tags passivos, semi-passivos e readers	http://www.alientechnology.com
Avery Dennison	Tags Gen1 e Gen2	http://www.RFID.averydennison.com
Biomark	Antenas, tags e readers	http://www.biomark.com
Brooks Automation	Antenas e readers	http://www.awid.com
Cofidex	Tags passivos e interrogadores	http://www.confidex.fi
Datamax Corporation	Tags, readers, impressoras	http://www.datamaxcorp.com
Ensyc	Dispositivos reader/writer	http://www.ensycRFID.com
FEIG	Readers, impressoras	http://www.feig.de
Impinj	Tags e readers	http://www.impinj.com
Intermec	Tags, readers, antenas e impressoras RFID	http://www.intermec.com
Omron	Antenas, tags e readers	http://www.omronRFID.com
Organic	Tags passivos orgânicos	http://www.organicid.com
Paxar	Tags passivos, smart Labels e Impressoras RFID	http://www.paxar.com
Philips	Tags e readers	http://www.philips.com
Printronix	Impressoras RFID	http://www.printonix.com
Psion Teklogix	Readers e impressoras RFID	http://www.psionteklogix.com
Reva Systems	Processadores de aquisição de dados de RFID	http://www.revasystems.com
RF	Code Tags e readers	http://www.rfcode.com
Sato	Tags, readers e impressoras RFID	http://www.satoamerica.com
SAVR	Communication Tags e readers	http://www.savrcom.com
Symbol	Tags, readers, inlays e até mesmo portais completos prontos a instalar	http://www.symbol.com
TagSys	Todo o tipo de material	http://www.tagsysRFID.com
Texas Instruments	Todo o tipo de produtos	http://www.ti.com/RFID
Zebra	Todo o tipo de dispositivos relacionados com RFID	http://www.zebra.com

Anexo B. Base de dados dos activos ATEC

Neste anexo estão descritos alguns dos activos presentes na base de dados, cujos nomes intermédios foram ocultados para garantir privacidade aos mesmos.

T_UTILIZADORES		
Nome	**Número do formando**	**Turma**
ALEXANDRE FONTOURA TEIXEIRA	10000101	GRP_07.06
ANDRÉ CORREIA DA FONSECA	10000102	GRP_07.06
ANDRÉ DA SILVA FAUSTINO	10000103	GRP_07.06
BRUNO ROCHA E SILVA	10000104	GRP_07.06
BRUNO DA SILVA CHAVES	10000105	GRP_07.06
CARLOS ESTRELA FERREIRA	10000106	GRP_07.06
CRISTOVÃO SILVA PEREIRA	10000107	GRP_07.06
DANIEL DIAS DOS SANTOS	10000108	GRP_07.06
IVO REINA DE SÁ COUTO	10000109	GRP_07.06
JOÃO OLIVEIRA RIBEIRO COUTO	10000110	GRP_07.06
JOÃO LUCAS CHIBANTE	10000111	GRP_07.06
JORGE SALGUEIRO CONCEIÇÃO	10000112	GRP_07.06
LUÍS FERREIRA DE JESUS	10000113	GRP_07.06
MANUEL FERREIRA RODRIGUES	10000114	GRP_07.06
PEDRO CONCEIÇÃO GASPAR	10000115	GRP_07.06
RICARDO SILVA SANTOS	10000116	GRP_07.06
SÉRGIO COSTA SILVA	10000117	GRP_07.06
SÉRGIO GONÇALVES MORTÁGUA	10000118	GRP_07.06
ADRIANA SILVA OLIVEIRA	10000201	TEIP_10.06
ANDRÉ MARTINS CARDOSO	10000202	TEIP_10.06
CRISTIANO BARBOSA PEREIRA	10000203	TEIP_10.06
DUARTE MARTINS CRISTINO	10000204	TEIP_10.06
FÁBIO DA SILVA GONÇALVES	10000205	TEIP_10.06
GILBERTO DA SILVA PEREIRA	10000206	TEIP_10.06
IVO DA SILVA E SOUSA	10000207	TEIP_10.06
JORGE SILVA RIBEIRO	10000208	TEIP_10.06
LUÍS PEDROSA DA SILVA	10000209	TEIP_10.06
PEDRO VIEIRA MEIRELES	10000210	TEIP_10.06
PEDRO ALVES RIBEIRO	10000211	TEIP_10.06
RICARDO MENDES LAGO	10000212	TEIP_10.06
SÉRGIO CARVALHO MENDES	10000213	TEIP_10.06
TIAGO OLIVEIRA PASSOS	10000214	TEIP_10.06
YANNICK DE JESUS VARINO	10000215	TEIP_10.06
DANIEL PEREIRA DA SILVA	10000301	TECP_10.06

T_UTILIZADORES		
Nome	**Número do formando**	**Turma**
FRANCISCO DE SOUSA BRITO	10000302	TECP_10.06
FRANCISCO GÓIS AUGUSTO	10000303	TECP_10.06
HÉLDER NASCIMENTO NUNES	10000304	TECP_10.06
HUGO FERNANDES DE SOUSA	10000305	TECP_10.06
HUGO MANUEL FERREIRA	10000306	TECP_10.06
JOÃO SENA DE VASCONCELOS	10000307	TECP_10.06
JOÃO MARQUES LEMOS	10000308	TECP_10.06
JORGE NOGUEIRA DA SILVA	10000309	TECP_10.06
MÓNICA OLIVEIRA RIBEIRO	10000310	TECP_10.06
NUNO DA SILVA DOMINGUES	10000311	TECP_10.06
PAULO GÓIS AUGUSTO	10000312	TECP_10.06
RICARDO PAREDES LOURENÇO	10000313	TECP_10.06
ROGÉRIO RÊGO FERREIRA	10000314	TECP_10.06
RÚBEN COSTA BARBOSA	10000315	TECP_10.06
RUI OLIVEIRA DE AZEVEDO	10000316	TECP_10.06
SARA SANTOS DE ABREU	10000317	TECP_10.06
TIAGO DA SILVA QUEIRÓS	10000318	TECP_10.06
HUGO FIGUEIRAS GONÇALVES	10000319	TECP_10.06
BEATRIZ RODRIGUES PIRES	10000401	ARCIP_07.06
JOSÉ COSTA FERNANDES	10000402	ARCIP_07.06
JÚLIO FERNANDEZ FERREIRA	10000403	ARCIP_07.06
LÍDIA LADEIRA ANTUNES	10000404	ARCIP_07.06
LUÍS GORDETE FAUSTINO	10000405	ARCIP_07.06
NUNO VILHENA MARQUES	10000406	ARCIP_07.06
NUNO FERREIRA GOMES	10000407	ARCIP_07.06
NUNO ROLINHO DA SILVA	10000408	ARCIP_07.06
RICARDO OLIVEIRA SILVA	10000409	ARCIP_07.06
RICARDO FERREIRA SANTOS	10000410	ARCIP_07.06
RICARDO DA SILVA BERNARDO	10000411	ARCIP_07.06
RICARDO PEREIRA DA ROCHA	10000412	ARCIP_07.06
SÉRGIO GUIMARÃES DE JESUS	10000413	ARCIP_07.06
SÉRGIO BARBOSA LOPES	10000414	ARCIP_07.06
TERÊNCIO AGUSTINHO HIPÓLITO	10000415	ARCIP_07.06
TIAGO PEREIRA DA SILVA	10000416	ARCIP_07.06
TIAGO DA SILVA MOURA	10000417	ARCIP_07.06
TIAGO VALENTE ASSUNÇÃO	10000418	ARCIP_07.06
VITOR PACHECO VIEIRA	10000419	ARCIP_07.06
BRUNO NARCISO ANTUNES	10000501	GRP_03.07
CÂNDIDO LIMA PEREIRA	10000502	GRP_03.07
FERNANDO TEIXEIRA RODRIGUES	10000503	GRP_03.07
JOSÉ DA SILVA ARAÚJO	10000504	GRP_03.07
HÉLDER VILAS BOAS	10000505	GRP_03.07
HENRIQUE MIRANDA E VASCONCELOS	10000506	GRP_03.07
HUGO PESSOA DA SILVA	10000507	GRP_03.07
NUNO RAMOS MOREIRA	10000508	GRP_03.07
MANUEL FERREIRA RODRIGUES	10000509	GRP_03.07

T_UTILIZADORES		
Nome	**Número do formando**	**Turma**
RUI SILVA E SOUSA	10000510	GRP_03.07
TELMO FIGUEIREDO OLIVEIRA	10000511	GRP_03.07
TIAGO DIAS RODRIGUES	10000512	GRP_03.07
ANA ROCHA MARQUES	10000601	CECP_04.07
BRUNO DE LIMA MACHADO	10000602	CECP_04.07
DANIEL SOUSA CASTRO	10000603	CECP_04.07
DIANA MONTES GOMEZ	10000604	CECP_04.07
JACINTO RIBEIRO DE VASCONCELOS	10000605	CECP_04.07
JÚLIO VILARES DA SILVA	10000606	CECP_04.07
LUÍS COSTA COELHO	10000607	CECP_04.07
MANUEL SANTOS MOTA	10000608	CECP_04.07
SANDRO PINTO PINHEIRO	10000609	CECP_04.07
ANA MOREIRA BATISTA	10000701	FPQP_06.07
FILIPA CUNHA AMORIM	10000702	FPQP_06.07
ISABEL FERREIRA TEIXEIRA	10000703	FPQP_06.07
JOANA MORAIS CORVAL	10000704	FPQP_06.07
MAFALDA TEIXEIRA DA SILVA	10000705	FPQP_06.07
MARIA GOMES DOS CAMPOS	10000706	FPQP_06.07
MARTA AREIAS DA SILVA	10000707	FPQP_06.07
RICARDO PIRES DE ALMEIDA	10000708	FPQP_06.07
RITA CARDOSO RODRIGUES	10000709	FPQP_06.07
RUI BOTELHO DA SILVA	10000710	FPQP_06.07
SILVIA BARBOSA PEREIRA	10000711	FPQP_06.07
SÓNIA CUNHA DE CARVALHO	10000712	FPQP_06.07
TÂNIA DA SILVA LEANDRO	10000713	FPQP_06.07
FRANCISCO SOARES LIMA	10000714	FPQP_06.07
JOÃO SANTOS TAVARES	10001101	DIRECTOR
MANUEL ARAÚJO DANTAS	10001102	CTI
PAULO SANTOS MARTINS	10001103	CA
RICARDO MAGALHÃES GONÇALVES	10001104	CONSULTOR
LISETE ARAÚJO SANTOS	10001105	ADMINISTRATIVA
SILVIA SILVA MILHAZES	10001106	ADMINISTRATIVA
PAULO VILELA PEIXOTO	10001107	FORMADOR
PEDRO TEIXEIRA DE SÁ	10001108	FORMADOR
FERNANDO SILVA VASCONCELOS	10001201	FORMADOR
ANA PAULA CUNHA	10001202	FORMADOR
CLEMENTINO RAMOS OLIVEIRA	10001203	FORMADOR
DANIEL JORGE VALENTE	10001204	FORMADOR
IVA ALEXANDRA VIANA	10001205	FORMADOR
IVO MANUEL PEREIRA	10001206	FORMADOR
JOSÉ CARLOS SOUSA	10001207	FORMADOR
LUCIANA MATOS SILVA	10001208	FORMADOR
MAFALDA DA COSTA ACEBEY	10001209	FORMADOR
MANUEL FERNANDO GONÇALVES TEIXEIRA	10001210	FORMADOR
MARCO SANTOS MARTINS	10001211	FORMADOR
MARIA SILVA FERREIRA	10001212	FORMADOR

T_UTILIZADORES		
Nome	**Número do formando**	**Turma**
MÁRIO ESTEVES SILVA	10001213	FORMADOR
ORLANDO FIGUEIRAS	10001214	FORMADOR
PEDRO NEVES MARTINS	10001215	FORMADOR
VIRGÍNIA DA CUNHA PÔJO	10001216	FORMADOR
ZITA OLIVEIRA MARTINS	10001217	FORMADOR
DANIEL DIAS SANTOS	10001301	ESTAGIÁRIO

Referências Documentais

[1] IDC *Mobility & RFID 26th February* 2007

[2] GOMES, Hugo Miguel — *Construção de um Sistema RFID com fins de localização Especiais* Universidade de Aveiro 2007

[3] XAVIER, Fernando — *O que é o RFID?* Conceptia Consulting Portugal.

[4] SYBASE PORTUGAL — *RSC/RFID Solutions Center*. Outubro 2006

[5] GLOVER Bill & BHATT, Himanschu, Fundamentos de RFID, 2007

[6] CIENTISTASSOCIADOS — *RFID Supply Chain melhorando a eficiência da cadeia de Suprimentos* www.cientistassociados.com.br

[7] COSTA, Pedro Alexandre — *Framework e Hardware RFID para Rastreabilidade e Segurança* Link Consulting, SA Junho 2006

[8] FERREIRA, Cristina — *RFID ultrapassa barreiras e ganha mercado* Singapour Comunicação e Marketing

[9] IBM GLOBAL SERVICES — *RFID, melhor, mais rápido, mais eficiente* Integrated Technology Services Newsletter ITS Newsletter 19a Edicao Junho 2005

[10] SIDEN, Johan - *Remote Moisture Sensing utilizing Ordinary RFID Tags* IEEE Sensors 2007 Conference

[11] LEONG, Kin – *Miniaturization of Dual Frequency RFID Antena with High Frequency Ratio* IEEE 2007

[12] WILLIAMS, John – *Interoperable Internet Scale Security Framework for RFID Networks* ICDE Workshop 2008

[13] FAGUI, Liu – *Rule Match-An Important Issue In RFID Middleware* IEEE 2007

[14] WATKINS, Steve – *RFID Instrumentation in a Field Application* IEEE Region 5 Technical Conference April 2007

[15] SEONGJIN, Kim – *RFID Business Aware Framework for Business Process in the EPC Network* IEEE Computer Society 2007

[16] HAN, Min – *A Framework for Seamless Information Retrieval between an EPC Network and a Mobile RFID Network* IEEE 2006

[17] KETPROM, Urachada – *Closing Digital Gap on RFID Usage for Better Farm Management* Pigmet Proceedings August 2007

[18] BIRARI, Shailesh – *Mitigating the Reader Collision Problem in RFID Networks with Mobile Readers* IEEE 2005

[19] CUI, Jian – *Mobile Agent based Load Balancing for RFID Middlewares* ICACT February 2007

[20] WAGNER, J – *The Influence of Metal Environment on the Performance of UHF Smart Labels in Theory, Experimental Series and Practice* IEEE 2007

[21] MIN, Zhang – *A RFID-based Material Tracking Information System* IEEE 2007

[22] NIKITIN, Pavel – *Performance of RFID Tags with Multiple RF Ports* IEEE 2007

[23] HOSSAIN, Muhammad – *Consumer Acceptance of RFID Technology: An Exploratory Study* IEEE 2008

[24] SHI-CHO, Cha – *An Efficient and Flexible Way to Protect Privacy in RFID Environment with Licenses* IEEE April 2008

[25] SINGAPOUR – *Throttleman agarrou a oportunidade* Jornal Têxtil 2007

[26] LEE, Nam – *Evolution of RFID Applications and Its Implications: Normaization Perspective* PICMET 2007

[27] RANKY, Paul – *Engineering Management-Focused Radio Frequency Identification (RFID) Model Solutions* IEEE 2007

[28] PISELO, Thomas – *Shrinking the Supply Chain Expands the Return: The ROI of RFID in the Supply Chain* Alinean August 2006

[29] GRANCE, Tim – *Security Normas for the RFID Market* IEEE 2005

[30] KOVAVISARUCH, J – *Converging Technology in Society: Opportunity for Radio Frequency Identification (RFID) in Thailand's Transportation System* PICMET 2007

[31] GI OUG, Oh – *A Quality Evaluation Technique of RFID Middleware in Ubiquitous Computing* IEEE 2006

[32] NACCACHE, David – *RFID Malware, Truth vs. Myth* IEEE Security and Privacy 2006

[33] RFID Solutions Center – *State of the Art in RFID*, 2008

[34] HIANGJYN, Lee – *Privacy threats and issues in mobile RFID* IEEE 2006

[35] RIEBACK, Melanie – *Is Your Cat Infected with a Computer Virus?* IEEE 2006

[36] AZEVEDO, Susana – *O impacto da identificação por rádio frequência (RFID) no desempenho das empresas: uma proposta de modelo de avaliação* Grupo de Investigação FEDRA 2007

[37] ROSA, Luiz – *Aplicação do RFID na Cadeia Logística* Universidade de São Paulo 2006

[38] RAZA, Nadeem – *Applications of RFID Technology* The Institution of Electrical Engineers 1999

[39] Sybase – *Estado da Arte em RFID*, 2007

[40] MELO, Francisco – *A Evolução Tecnológica dos Normas RFID* IV Encontro Empresarial de Mobilidade e RFID 2008

[41] INNOVAGENCY- *Como funciona a Via Verde?*www.viaverde.pt 2008

Histórico

- 15 de Fevereiro 2008, Versão 1.0, mailto:1980337@isep.ipp.pt
- 25 de Fevereiro de 2008, Versão 1.0a, mailto:1980337@isep.ipp.pt
- 15 de Setembro de 2008, Versão 2.0, mailto:1980337@isep.ipp.pt
- 21 de Setembro de 2008, Versão 2.0a, mailto:1980337@isep.ipp.pt
- 25 de Setembro de 2008, Versão 2.0b, mailto:1980337@isep.ipp.pt
- 28 de Setembro de 2008, Versão 3.0, mailto:1980337@isep.ipp.pt
- 05 de Outubro de 2008, Versão 3.0a, mailto:1980337@isep.ipp.pt
- 07 de Outubro de 2008, Versão 3.0b, mailto:1980337@isep.ipp.pt
- 22 de Outubro de 2008, Versão 4.0, mailto:1980337@isep.ipp.pt
- 03 de Novembro de 2008, Versão 4.0a, mailto:1980337@isep.ipp.pt
- 09 de Novembro de 2008, Versão 5.0, mailto:1980337@isep.ipp.pt