Universidade de Aveiro
2009
Departamento de Engenharia Electrónica, Telecomunicações e Informática

Alírio de Jesus Soares Boaventura

Leitor/Gravador RFID – Banda HF (13.56 MHz)

Universidade de Aveiro
2009

Departamento de Engenharia Electrónica,
Telecomunicações e Informática

Alírio de Jesus Soares Boaventura

Leitor/Gravador RFID – Banda HF (13.56 MHz)

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia Electrónica e Telecomunicações realizada sob a orientação científica do Doutor Nuno Borges de Carvalho, Professor Associado do Departamento de Engenharia Electrónica, Telecomunicações e Informática e co-orientação do Doutor Pedro Miguel Lavrador, Professor Auxiliar Convidado do Departamento de Engenharia Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Dedico este trabalho aos meus pais Alfredo e Maria e aos meus irmãos José, Luísa e Rosa que sempre acreditaram em mim, e mesmo à distância me apoiaram incondicionalmente, provando que nem sempre é preciso estar perto para se marcar a diferença.

Júri

Presidente	**Doutor José Carlos Esteves Duarte Pedro** Professor Catedrático do Departamento de Engenharia Electrónica, Telecomunicações e Informática da Universidade de Aveiro
Vogal/Arguente	**Doutor Rafael Ferreira da Silva Caldeirinha** Professor Coordenador do Departamento de Engenharia Electrotécnica da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria
Vogal/Orientador	**Doutor Nuno Miguel Borges de Carvalho** Professor Associado do Departamento de Engenharia Electrónica, Telecomunicações e Informática da Universidade de Aveiro
Vogal/Co-orientador	**Doutor Pedro Miguel Lavrador** Professor Auxiliar Convidado do Departamento de Engenharia Electrónica, Telecomunicações e Informática da Universidade de Aveiro

Agradecimentos

Esta dissertação representa o auge de uma etapa académica, razão pela qual a lista de agradecimentos se adivinha longa.

Em primeiro lugar gostaria de agradecer toda a minha família pelo apoio e incentivo em todas as etapas do meu percurso académico.

Não poderia deixar de agradecer aos meus amigos e colegas de caminhada, Igor Fonseca, João Ramos, Odracir Almeida, Irina Carvalho e João Cruz, acreditando que sem eles seria tudo mais difícil.

Um obrigado aos meus orientadores Professor Doutor Nuno Borges de Carvalho e Professor Doutor Pedro Miguel Lavrador pela orientação e total disponibilidade ao longo de todo o trabalho.

Na pessoa do Sr. Jorge Renato Graça gostaria de agradecer à Acronym pela oportunidade que me concederam de poder trabalhar com eles e pela sua colaboração em todas as fases do projecto.

A um grande amigo, que me ensinou a dar os primeiros passos em electrónica. Obrigado João de Deus Da Luz.

Aos amigos de longa data, Manuel Rocha, Widson Monteiro e Luís Oliveira, um grande obrigado pelo incentivo constante.

Um obrigado à Universidade de Aveiro pelas condições excepcionais de formação.

A todos aqueles que directa ou indirectamente contribuíram para levar este projecto a bom porto.

Por fim, gostaria de expressar a minha profunda gratidão à Fundação Calouste Gulbenkian pela bolsa de estudos que me foi concedida durante o período de formação universitária.

Palavras – chave

RFID, tecnologia passiva, cartões sem contacto, norma ISO14443-A, Mifare Standard (NXP)

Resumo

Esta dissertação surge no âmbito de uma parceria com a empresa Acronym, Informação e Tecnologia e visa o projecto e desenvolvimento de um leitor/gravador RFID para a banda HF (13.56MHz). O trabalho aqui desenvolvido centra-se essencialmente nas camadas física e MAC referentes à norma ISO14443 – Cartões de Identificação – Cartões sem contacto de proximidade.

Uma vez projectado e integrado o hardware, passou-se ao desenvolvimento do firmware que implementa o protocolo ISO14443-A. Foi também criada uma interface simples (Hyperterminal/RS232) que permita ao utilizador, entre outras operações, gravar/ler blocos de dados do transponder.

Keywords RFID, passive technology, contactless smart cards, ISO14443-A standard, Mifare Standard (NXP)

Abstract

This Thesis is developed in cooperation with Acronym, Informação e Tecnologia Company. The main goal is project an RFID reader/writer device working in the HF band (13.56MHz). We're working around the ISO14443-A protocol (Contactless integrated circuit(s) cards – Proximity cards) and we are focused in the Physical and Medium Access Control layer.

Once all the hardware was integrated, the firmware that supports the ISO14443-A protocol was created. A simple user interface using HyperTerminal/RS232 was developed in order to allow user to access the transponder memory.

Índice

Índice de figuras

Índice de tabelas

Lista de acrónimos

RFID – Radio Frequency Identification

LF – Low Frequency

HF – High Frequency

UHF – Ultra High Frequency

MAC – Medium Access Control

NFC – Near Field Communication

UID – Unique IDentifier

SPI - Serial Peripheral Interface Bus

MCU – Micro Controller Unit

RISC – Reduced Instruction Set Computers

CRC – Cyclic Redundancy Check

EAS – Electronic Article Surveillance

EPC – Electronic Product Code

UPC – Universal Product Code

POR – Power On Reset

SDR – Software Defined Radio

REQA – REQuest All

ATQA – Answer To reQuest

ETU – Elementary Time Unit

DSP – Digital Signal Processor

Capítulo 1 – Introdução

1.1 – Motivações e Objectivos

A identificação por radiofrequência (RFID) parece ser uma tecnologia que não conhece limites quanto ao número e variedade de aplicações. Recentemente o número de etiquetas e cartões electrónicos sem contacto tem crescido significativamente. Esta tecnologia tem sido utilizada largamente em logística (catalogação e rastreamento de produtos), veículos e portagens, sistemas anti-roubo, controlo de acesso e assiduidade, pagamento electrónico e cartões de fidelização, autenticação, sistemas de localização e mais recentemente em passaportes, telemóveis (NFC) e até para "identificação biométrica", sendo implantado no próprio corpo humano.
Casos pioneiros de sucesso nacional a serem apontados são o da Throttleman (aplicação de RFID ao processo logístico na indústria de retalho), o da Brisa (RFID aplicado à cobrança e controle de portagens) e o do metro do Porto e de Lisboa.
Actualmente, a padronização em RFID existe e é estável. Por outro lado a indústria dos semicondutores tem desenvolvido soluções altamente integradas capazes de implementar diversos protocolos com relativa facilidade e reduzido esforço de desenvolvimento. São exemplos disso, os transceivers RFID HF "MFRC531" da NXP (utilizado neste projecto), RFID HF "TRH031M" da 3ALOGICS e RFID UHF "R1000" da Intel. Isto, para dizer que surgem novas oportunidades de desenvolvimento e integração para a industria manufactora.
A **Acronym, Informação e Tecnologia**, é uma empresa especializada em software de gestão de tempos e relógios de ponto que também desenvolve as suas próprias soluções de recolha de dados. Uma das suas apostas é a identificação por rádio, onde já possui uma solução em LF (125 kHz) para cartões sem contacto e pretende lançar para o mercado uma nova solução em HF. Para além da maior diversidade de produtos, esta solução traz as vantagens de maior espaço de armazenamento (tag com até 4KBytes memória), maior alcance (até 10 cm sem amplificação externa) e maior interoperabilidade uma vez que opta-se por usar transponders de um dos maiores fabricantes mundiais, a NXP.
É portanto, objectivo desta dissertação, em colaboração com a Acronym, projectar um leitor/gravador RFID para a banda HF (13.56MHz). Para isto recorre-se a um transceiver RFID HF da NXP que constituirá o *core* do leitor. Os transponders a utilizar neste projecto são igualmente da NXP Semiconductors. Trata-se da família de cartões sem contacto

Mifare (standard 1KByte, standard 4KByte e UltraLigth). Esta escolha deve-se ao facto da NXP ser actualmente um dos maiores fabricantes mundiais de cartões electrónicos sem contacto.
"NXP's MIFARE contactless technology is widely deployed for transport networks and access management worldwide. With more than one billion cards in circulation today, MIFARE platforms are the most widely deployed contactless technology. The availability of MIFARE-compatible applications on mobile phones further strengthens the attractiveness of the NFC technology."[1]
"The mifare Classic is the most widely used contactless smart card in the market." [2]
A corroborar as citações anteriores, consta o facto de o novo cartão universitário da Caixa Geral de Depósitos incorporar um chip RFID da Mifare.
Finalmente, convém dizer que outros requisitos, não menos importantes, são tidos em conta ao longo deste projecto procurando-se chegar a uma solução final fiável, de reduzidas dimensões, elevada integração e baixo custo.

1.2 – Estrutura da dissertação

Esta dissertação encontra-se dividida em seis capítulos. O primeiro capítulo introduz a dissertação procurando enquadrar as motivações e objectivos da mesma no panorama actual da tecnologia RFID.
O segundo capítulo constitui um estudo do "estado da arte" da tecnologia RFID. Neste capítulo começa-se por fazer um resumo histórico da tecnologia evidenciando os principais marcos que concorreram para a existência da tecnologia tal como a conhecemos hoje. Prossegue-se com um estudo tecnológico, onde se abordam aspectos como a composição do sistema, aplicabilidade da tecnologia, classificação dos sistemas RFID, frequências de operação, potências, alcance, codificação e modulação. É também feito um levantamento das principais normas e standards existentes dando ênfase ao standard ISO14443-A (utilizado neste projecto) e ao protocolo EPC da EPCGlobal inc. Seguidamente, é feita alusão a algumas questões éticas ligadas à tecnologia. A finalizar, apresenta-se uma análise mais detalhada dos princípios de funcionamento de alguns dos sistemas passivos mais utilizados. Analisa-se aqui o sistema EPC-*backscatter modulation*, o sistema EAS por efeito não linear e finalmente os cartões electrónicos sem contacto por acoplamento indutivo.
O capítulo terceiro aborda os aspectos relevantes do hardware. Neste capítulo faz-se o dimensionamento e adaptação da antena do leitor bem como a integração de todo o hardware necessário.
A discussão do código desenvolvido neste projecto é feita no capítulo quatro. Começa-se por descrever a estrutura do código e a sincronização da comunicação aplicação-leitor e leitor-transponder. Posteriormente pormenoriza-se toda a implementação do protocolo ISO14443-A e faz-se uma breve descrição de todas as funções desenvolvidas. A finalizar o capítulo, apresenta-se a aplicação de demonstração desenvolvida.
Medidas e testes merecem atenção no capítulo cinco, onde é verificada a conformidade dos sinais de interface com a parte 2 do standard ISO14443A. Adicionalmente é feito um estudo experimental do comportamento de diversas antenas (formato, número de espiras e material) sob o efeito de carga do transponder, de modo a escolher-se a mais adequada.

Finalmente é feito um estudo do efeito de alguns materiais no alcance de leitura, quando interpostos entre o leitor e o tag.
O sexto e último capítulo dedica-se à análise e conclusões do trabalho levado a cabo neste projecto e à apresentação de propostas de trabalho futuro.

Capítulo 2 – Introdução aos Sistemas RFID

O que é o RFID?

RFID, do Inglês – *Radio Frequency Identification*; em Português – Identificação por Rádio Frequência;
É um método de identificação automática, que recorre a sinais rádio para ler e gravar dados, de forma remota, num dispositivo de armazenamento denominado transponder [3][4][5]. Permite a identificação única, o rastreamento e localização de pessoas, animais e objectos, usando sinais rádio.

2.1 – História

Acompanhando a evolução das telecomunicações, a tecnologia RFID tem vindo a afirmar-se como a nova geração de sistemas de identificação automática. O facto de não exigir contacto físico ou linha de vista entre o leitor e o transponder e os elevados débitos de dados são algumas das principais razões que a colocam em vantagem face as demais técnicas de ID automático.
O conceito de RFID teve a sua origem nos sistemas de radares utilizados na segunda guerra mundial. Nesta altura, os alemães, japoneses, americanos e ingleses utilizavam radares (descobertos em 1935 por Robert Alexander Watson-Watt, físico escocês) para detectar a aproximação de aviões. Estes sistemas cumpriam com as especificações para que haviam sido criados (detectar a aproximação de aviões), no entanto, havia um grande problema: como distinguir entre aviões inimigos e aliados? Os alemães descobriram então que, se os seus pilotos girassem os aviões quando regressavam à base, modificariam as características do sinal de rádio reflectido. Esse método simples permitia aos alemães reconhecer os seus aviões. Este pode ser considerado o primeiro sistema RFID passivo [3]
O primeiro identificador activo foi desenvolvido pelos ingleses (com a colaboração de Robert Alexander Watson-Watt). Trata-se do sistema IFF- *Identify Friend or Foe*, que significa identificador de amigo ou inimigo. Foram colocados transceivers nos aviões britânicos que respondiam aos sinais da estação base com um identificador "amigo" [4]. Este é o conceito utilizado nos sistemas RFID modernos. O leitor faz o *broadcast* do sinal rádio, este sinal é recebido pelo transponder que o reflecte (sistemas passivos) ou transmite um sinal próprio (sistemas activos). A Fig.1 mostra a evolução da tecnologia RFID ao longo dos tempos [6].

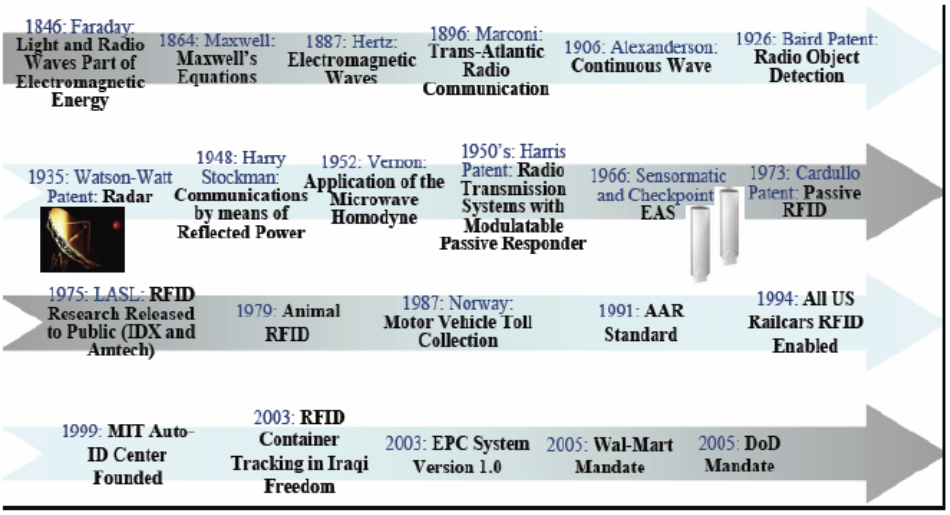


Fig. 1) História do RFID, retirado de [6]

Passa-se a realçar alguns dos marcos mais importantes: em 1846 o inglês Michael Faraday descobre que tanto a luz como as ondas rádio são parte do espectro electromagnético;
Em 1864, James Clerk Maxwell (físico escocês) publica as equações sobre o campo electromagnético – Leis de Maxwell.
Em 1887, Heinrich Rudolf Hertz (físico alemão) confirma as leis de Maxwell com um estudo sobre ondas electromagnéticas. Hertz é o primeiro cientista a conseguir transmitir e receber ondas de rádio.
Em 1896, Guglielmo Marconi consegue efectuar a primeira transmissão de informação via rádio, naquela que seria a primeira comunicação transatlântica sem fios.
Já em 1948, o trabalho de Harry Stockman intitulado "*Comunnication by Means of Reflected Power*"explorou o uso de potência reflectida como meio de comunicação [7].
Na década de 60 a tecnologia avança significativamente. Diversos estudos sobre a teoria e modo de funcionamento do sistema impulsionam na década seguinte, o advento da tecnologia tal como a conhecemos hoje. Entre esses avanços, destacam-se os estudos sobre a teoria electromagnética relacionada com o RFID, efectuados por R. F.Harrington [8].

Em 1973, surge a primeira patente sobre o RFID requerida por Mário W. Cardullo. Trata-se de um sistema activo com memória reprogramável.
A partir da década de 80, o RFID entra definitivamente na indústria e no mercado mundial. São abertos centros de Investigação e Desenvolvimento um pouco por todo o mundo. Na década de 90 começam a surgir as primeiras normas e standards sobre RFID.
Em 1999 foi criado o centro de identificação automática do MIT, o MIT Auto-ID Center que lançou em 2003 a primeira versão do sistema EPC, um sistema pensado para substituir o código de barras (UPC). A tabela 1 resume a evolução do RFID ao longo das décadas [8].

Década	Acontecimento
1940-1950	Invenção e desenvolvimento do radar durante a 2ª guerra mundial Surgimento do conceito de RFID
1950-1960	Primeiras experiências laboratoriais em RFID
1960-1970	Desenvolvimento da teoria do RFID Primeiras aplicações práticas
1970-1980	Expansão no desenvolvimento do RFID Aceleração dos testes Implementações embrionárias de RFID
1980-1990	Aplicações comerciais de RFID no mercado
1990-2000	Surgimento de normas e standards RFID utilizado em larga escala Criação do centro de investigação do MIT
2000…	Primeira versão do sistema EPC NFC – RFID nos telemóveis Nokia testa o telemóvel Nokia 3220 compatível com NFC em transportes públicos (Alemanha-2005) [9]

Tabela 1) Evolução da tecnologia RFID ao longo das décadas

Actualmente, a tecnologia RFID atingiu uma maturidade notável. Conhece um vasto leque de aplicações e está presente no nosso quotidiano.

2.2 – Componentes básicos de um sistema RFID

A Fig.2 mostra a constituição básica de um sistema RFID. Os principais componentes são: leitor e Antena, transponder, e Servidor de aplicação (PC). Através da sua antena o leitor faz a difusão do sinal rádio, interrogando todos os transponders que se encontrarem no seu campo. Num sistema "*reader talks first*", esta é a primeira operação a ter lugar. Dependendo do tipo de sistema em causa (passivo ou activo), o transponder no campo do leitor fará ou não uso do campo recebido para se alimentar, período após o qual o transponder estará pronto para iniciar transacções com o leitor.
Nos sistemas mais simples, o transponder após receber o sinal do leitor responde (por reflexão) com o seu UID. Já nos mais complexos são necessárias mais algumas etapas até que o transponder possa devolver o seu UID e/ou conteúdo de memória.
Em geral, o leitor RFID está conectado a um servidor com maior poder de processamento responsável pela aplicação principal do sistema.

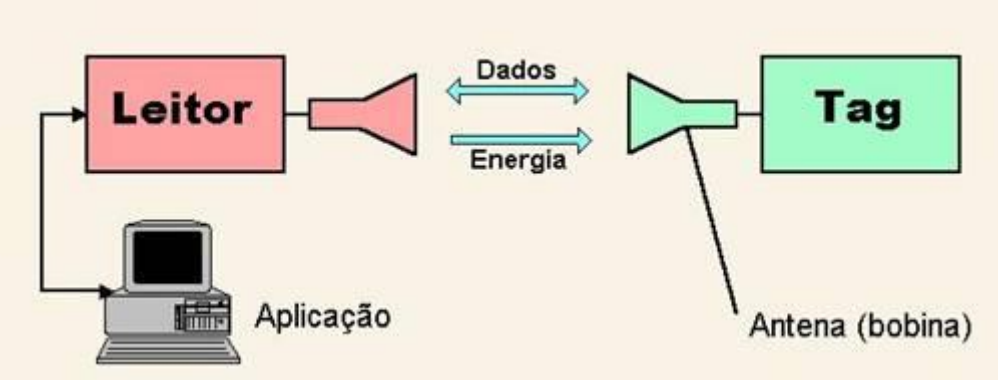


Fig. 2) Componentes básicos de um sistema RFID, retirado de [6]

2.3 – Aplicações, aplicabilidade e ética

Actualmente, é vasto e variado o leque de aplicações da tecnologia RFID, indo desde a simples identificação de bens, pessoas e animais a sistemas de navegação e localização em ambientes internos. De entre as aplicações mais comuns destacam-se as seguintes:

- Identificação de pessoas e animais
- Controle de acessos e assiduidade
- Autenticação
- Sistemas de pagamento electrónico
- Cartões de fidelização
- Controle e pagamento de portagens
- Sistemas anti-roubo
- Rastreamento e localização de produtos…

Parece ser interminável a lista de aplicações desta tecnologia. Esta situação acentua-se ainda mais, se pensarmos no RFID como o substituto " ideal" do código de barras e da banda magnética. Isto é, tudo o que já fazia a banda magnética e o código de barras, fá-lo melhor o RFID com muitos acrescentos. No entanto, há um senão importante a ter-se em conta, o custo. O custo ainda relativamente elevado da tecnologia não justifica a sua aplicação em alguns segmentos de mercado. Tomemos como exemplo a catalogação de produtos num estabelecimento comercial. Se por um lado, há produtos que pelo seu preço (da ordem do preço do transponder) não justificam o investimento, por outro, a cobertura de uma grande área implicaria um elevado número de leitores e logo um elevado custo.
Assim sendo, apenas uma aposta por parte da indústria (semicondutora e manufactora) em soluções RFID *low cost* potenciará o uso massificado, fazendo do RFID o substituto inevitável do código de barras. Convém dizer que há cada vez mais investigação e desenvolvimento neste sentido. Em 2003 o MIT Auto-ID Center criou o sistema EPC (Fig. 1). Este sistema foi desenhado para substituir o código de barras (UPC) e conta actualmente com três versões melhoradas. Uma abordagem mais detalhada do sistema EPC será feita nas secções 2.7.2 (O protocolo EPC Global) e 2.8.2 (Sistema EPC – *Backscatter Modulation*).

Outra tentativa de viabilizar a competição entre o RFID e o código de barras foi o sistema I-Code desenvolvido pela NXP. Trata-se de um sistema de vizinhança (distâncias de leitura até 1m) criado com o intuito de minimizar tanto quanto possível o preço das etiquetas [10] e destina-se à catalogação de grandes volumes de itens.
Em oposição ao exemplo anteriormente apontado, onde a aplicabilidade do RFID não é de todo evidente, há inúmeros casos em que a sua aplicação, em detrimento de outros sistemas de ID, é inteiramente justificada e vantajosa. Trata-se de situações em que, por exemplo, se queira catalogar, rastrear e localizar bens valiosos, sem linha de vista e sob condições adversas. Um exemplo ilustrativo foi o uso da identificação por radiofrequência durante a guerra do Iraque (2003 – 2004) por parte das forças da coligação para a monitorização de equipamento militar.

Um assunto muito discutido actualmente prende-se com a validade ética da tecnologia RFID e da forma como esta é aplicada. Realmente, uma utilização abusiva e indevida pode não só pôr em causa a privacidade do indivíduo como a segurança dos seus dados. No entanto, estas ameaças não invalidam todas as vantagens que esta tecnologia coloca ao nosso dispor. Por exemplo, a Internet, esta ferramenta quase indispensável no nosso dia-a-dia, é utilizada para muitas finalidades menos boas. Ainda assim, está cada vez mais presente e com um papel central na sociedade da informação.
No caso da utilização da tecnologia RFID na identificação e nos cartões inteligentes, a principal preocupação está relacionada com o facto do transponder poder ser "lido" à distância, sem o conhecimento/consentimento do indivíduo, o que na melhor das hipóteses constitui uma violação da sua privacidade. Convém, no entanto, dizer que esta situação pode ser contornada com mecanismos de segurança de dados na interface ar como autenticação do leitor e encriptação de dados.
No caso do uso da tecnologia para catalogação de produtos e bens, em muitos casos o comprador não está devidamente informado sobre a presença do dispositivo no produto que compra, tão pouco é capaz de removê-lo. Por outro lado, uma vez que as etiquetas podem não ser desactivadas após a compra, estas podem ser utilizadas de forma imoral para acompanhar as pessoas e os seus comportamentos. Esta é uma questão que a tecnologia em si não pode resolver. A tecnologia proporciona um conjunto de vantagens, e como tudo, traz associado algumas contrapartidas menos favoráveis. A partir daí há que discutir e criar um código ético e apelar ao bom senso das partes envolvidas.

2.4 – Classificação dos sistemas RFID

A classificação dos sistemas RFID é muito mais vasta do que aquela que aqui se apresenta. Faz-se aqui uma diferenciação dos sistemas segundo os critérios que se julgam mais relevantes tais como forma de alimentação do transponder, natureza do campo utilizado (magnético ou electromagnético), capacidade de armazenamento de dados e técnica de *downlink/uplink* de dados. Esta diferenciação poderia, no entanto, ser estendida a outras características.

2.4.1 – Forma de Alimentação do transponder

Quanto à forma de alimentação do transponder os sistemas podem ser classificados como activos, passivos ou semi-activos (ou semi-passivos).

Sistemas Passivos

Neste tipo de sistemas o transponder não possui uma fonte de energia própria. O transponder serve-se do campo magnético/electromagnético proveniente do leitor para se alimentar. Este tipo de dispositivos é, em geral, mais compacto que um transponder activo, mais barato e não carece de manutenção, possuindo, no entanto, um menor alcance.
Um sistema passivo é sempre do tipo "*Reader Talks first*", uma vez que o *tag* precisa do campo do leitor para se alimentar.
Para além do chip e da antena, um transponder passivo possui um rectificador e um regulador de tensão para extrair potencia DC do sinal RF, potencia essa que irá alimentar a electrónica interna do chip. Na Fig. 3 está representado o diagrama de blocos típico de um transponder passivo.

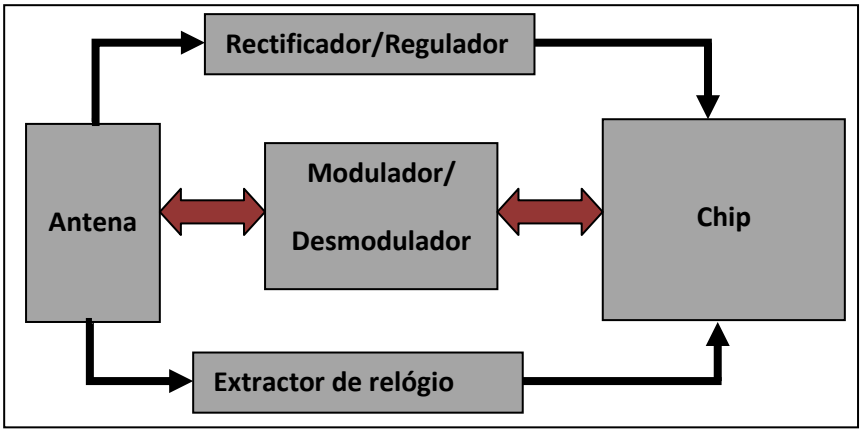


Fig. 3) Diagrama de blocos - Tag passivo

Aqui, a antena tem a função adicional de aproveitar a energia do campo recebido para alimentar o chip, razão pela qual o alcance do sistema depende muito do formato e tamanho da mesma.
Na figura seguinte mostram-se vários *tags* passivos com formatos de antena diferentes. O primeiro é um *tag* com acoplamento magnético (a antena é uma simples bobina) e os restantes são *tags* com acoplamento electromagnético. O formato da antena varia consoante a aplicação, frequência de operação e alcance máximo pretendido.

Fig. 4) Transponders Passivos

Sistemas Activos

Nestes sistemas o transponder tem a sua própria fonte de energia interna (baterias), não precisando da energia proveniente do leitor para se alimentar. Isto permite maior complexidade e independência do transponder. Os transponders activos normalmente têm maior alcance e maior capacidade de armazenamento que os passivos, no entanto, apresentam a contrapartida de ser necessário repor a bateria ocasionalmente.
São capazes de realizar tarefas complexas, como por exemplo, entrar em modo de poupança de energia quando não se encontram no campo do leitor. O facto de serem energeticamente independentes permite usá-los em configuração de sensores de medida para monitorizar, em modo *offline*, por exemplo, uma temperatura e comunicar os valores ao leitor quando este for ligado.
Em geral, os transponders activos são mais caros que os passivos e necessitam de manutenção (troca de bateria) ocasional.
A Fig. 5 mostra dois tags activos, um dos quais possui uma antena externa, o que maximiza o seu alcance.

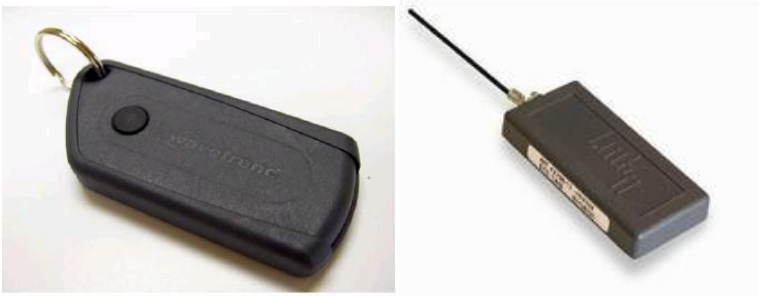


Fig. 5) Exemplo de transponder Activo

Sistemas Semi-passivos (Semi-activos)

Neste tipo de sistemas o transponder possui uma fonte de energia interna que serve apenas para alimentar a electrónica interna de controlo, mas não para gerar qualquer potência RF própria. Para a comunicação RF, é utilizado o mesmo princípio dos sistemas passivos, a

reflexão de potência [11]. Este sistema representa um compromisso entre os sistemas passivo e activo, permitindo um maior alcance que nos passivos e um maior tempo de vida da bateria que nos activos.

2.4.2 – Natureza do campo utilizado (M ou EM)

Quanto à natureza do campo utilizado na interface ar, os sistemas RFID podem ser divididos em dois grupos. Sistemas com acoplamento indutivo e sistemas com acoplamento electromagnético. Esta diferenciação tem a ver com a componente do campo utilizada para comunicação. A Fig. 6 mostra, à esquerda, um sistema com acoplamento indutivo e à direita um sistema com acoplamento electromagnético. Num sistema indutivo, apenas a componente magnética (B) do campo electromagnético é utilizado. O princípio de transferência de dados/energia neste tipo de sistemas é semelhante ao de um transformador em que as antenas do leitor e do transponder podem ser vistas respectivamente como primário e secundário de um transformador. Estes sistemas operam nas bandas LF (100-135kHz) e HF (10 -15MHz). As antenas são simples bobinas, uma vez que, a estas frequências uma antena convencional seria impraticável.
Já num sistema com acoplamento electromagnético a informação/energia é transportada por ondas de rádio. Em geral, os sistemas com acoplamento electromagnético operam na banda UHF (800-900MHz e 2.4GHz). Nestas faixas de frequências os comprimentos de onda são bastante baixos permitindo a construção de antenas de reduzidas dimensões e elevada eficiência.

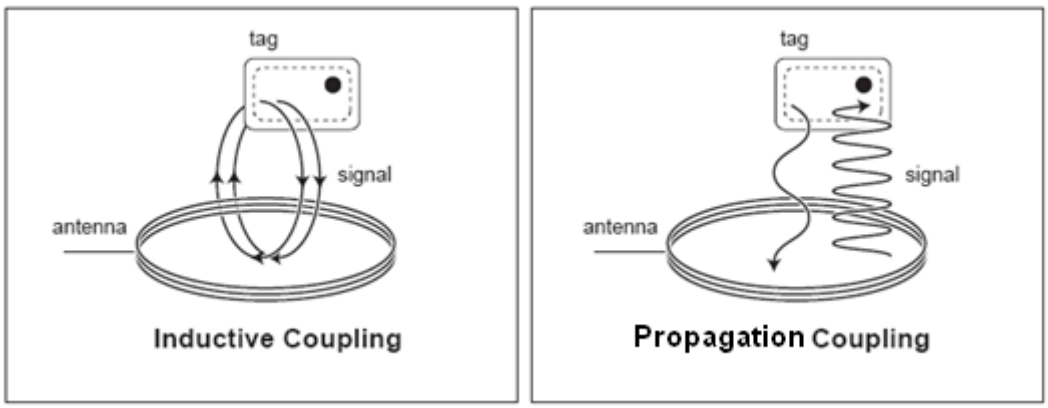


Fig. 6) Tipo de comunicação, adaptado de [11]

2.4.3 – Capacidade de armazenamento e reprogramabilidade

No tocante ao armazenamento de dados, uma primeira subdivisão pode ser feita em relação à quantidade de dados que o transponder pode armazenar. Temos essencialmente dois grupos: Sistemas 1 bit – transponder e Sistemas N bits – transponder.
Nos sistemas 1 bit – transponder, há apenas dois estados possíveis: "*tag in the field*" e "*no tag in the field*". O primeiro estado indica a presença de pelo menos um transponder no campo de leitura enquanto o segundo estado indica a inexistência de transponders no

campo de leitura. Em alguns sistemas, há ainda a possibilidade de desactivar o transponder, apagando a sua memória.
Os sitemas 1 bit – transponder são utilizados em situações em que apenas se quer saber, sem redundância adicional, se o transponder "está" ou "não está" no campo. Os sistemas anti-roubo EAS utilizados em estabelecimentos comerciais são disso um bom exemplo. Nestes casos, apenas se quer saber se um produto, seja ele qual for, saiu do estabelecimento de forma ilícita. No sistema EAS há a possibilidade de desactivar o transponder, visto que, uma vez o produto vendido, este não mais deverá ser detectado pelo sistema. O princípio de funcionamento do sistema EAS será discutido em detalhe na secção 2.8.1. Em geral, os sistemas 1 bit – transponder são passivos.
Nos sistemas N bits – transponder, o transponder possui uma memória capaz de armazenar dados desde alguns bytes até alguns Kbytes. Estes dados podem ser simplesmente o número de série do dispositivo (etiquetas RFID para catalogação de produtos) ou dados do utilizador (*smart cards contactless*). Neste caso há, de facto, comunicação de dados entre leitor e transponder podendo a transferência de dados ser do tipo *full duplex, half duplex* ou sequencial. Estas formas de comunicação serão abordadas na secção seguinte. Um sistema N bits - transponder tanto pode ser passivo ou activo.
Quanto ao tipo de memória utilizado, os transpoders podem subdividir-se em três grupos:

- ***Read Only*** (RO)
- ***Write Once Read Many*** (WORM)
- ***Read Write*** (RW)

Transponders RO apenas permitem a leitura de dados da sua memória. Este tipo de dispositivo é programado no fabrico com uma identificação única (número de série) não sendo, posteriormente, possível gravar ou apagar dados da sua memória. Como exemplo temos o sistema EPC que destina-se à catalogação de itens em lojas, bibliotecas ou aeroportos. Cada etiqueta EPC possui um UID de 64 bits (8 bytes), que para efeitos práticos, garante a unicidade das etiquetas [12]. Normalmente num sistema RO há sempre uma base de dados que faz a associação do UID com informação adicional (preço de produto, nome de utilizador, proprietário de bagagem).
Um transponder WORM é em tudo idêntico a um RO, com a diferença de haver a possibilidade de uma primeira e única gravação do *tag*, que poderá ser feita pelo utilizador final.
Os transponders RW permitem a leitura e escrita inclusivamente a reprogramação *online* (no campo) por um leitor/gravador autorizado. Alguns transponders podem também gravar informação dinâmica como temperatura, humidade ou localização. Os transponders RW mais sofisticados (activos) funcionam como computadores sem fios, permitindo a comunicação inter-*tag* ou até mesmo a conexão à internet [12]. A figura seguinte faz uma relação entre a capacidade de memória (transponders N bits - Transponder), a reprogramabilidade e outras funcionalidades dos transponders actuais.

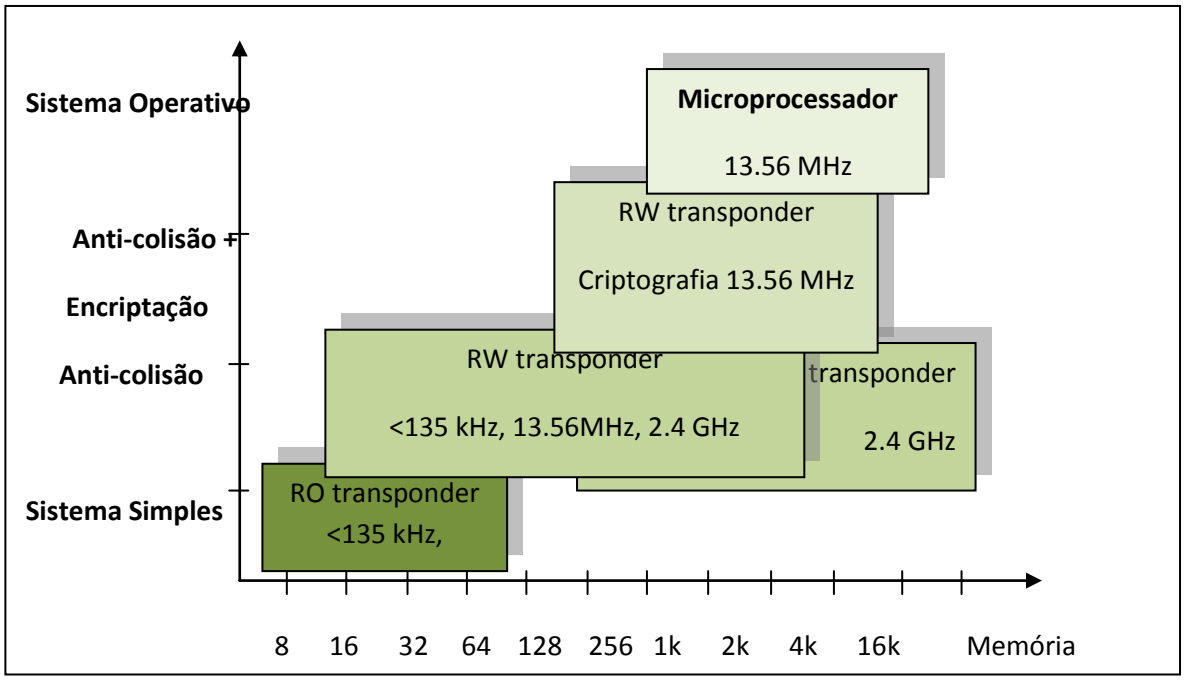


Fig. 7) Capacidade de armazenamento, adaptado de [5]

2.4.4 –Transmissão de dados

Esta diferenciação está relacionada com a transmissão de dados e energia entre o leitor e transponder e com a forma como esta se faz no tempo. Ao contrário dos sistemas 1-bit em que apenas há uma reacção física por parte do tag, normalmente uma oscilação ou um efeito não linear, nos sistemas N-bits há realmente uma transferência de dados. Esta transacção pode-se fazer de três formas distintas: *full duplex*, *half duplex* e sequencial (Fig. 8).

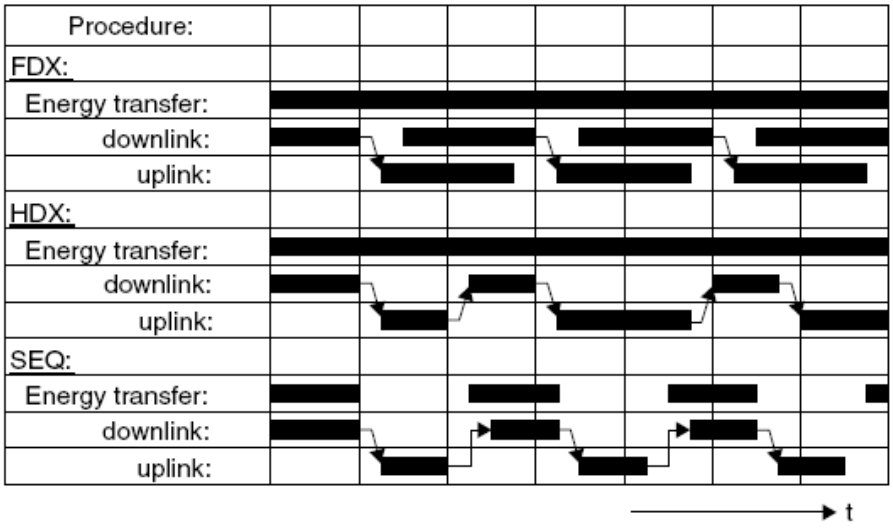


Fig. 8) Transmissão *full duplex,half duplex* e sequencial, retirado de [5]

Na transmissão *full duplex* (FDX), a informação é enviada nos dois sentidos (*downlink* e *uplink*) em simultâneo. Este tipo de transacção permite um maior débito de informação por unidade de tempo, uma vez que tanto o leitor como o transponder operam ao mesmo tempo como transmissor e receptor. Um exemplo mais geral de transmissão FDX é o protocolo SPI. O SPI utiliza dois buffers (um no transmissor e outro no receptor) que permutam os dados neles presentes de forma simultânea. Nos sistemas RFID FDX, a transferência de energia (sistemas passivos) acontece de forma continua. Um sistema RFID FDX pode ser visto num sistema por sub-harmónicas. Neste sistema o transponder responde com uma fracção da frequência recebida do leitor. Uma vez que o transponder serve-se da oscilação do leitor para responder, as operações de *uplink* e *dowlink* deverão ser simultâneas.
Numa transmissão *half duplex* (HDX), a transmissão e recepção não é feita em simultâneo. Os dispositivos operam ora como transmissor ora como receptor. Tendo um dispositivo A e um B, se num dado instante A estiver a transmitir, B estará apenas a receber. Num instante posterior os papéis invertem-se, passando B a operar apenas como transmissor e A apenas como receptor. Também aqui a transmissão de energia é feita de forma continuada. Um exemplo de sistema HDX é o sistema indutivo de proximidade por modulação de carga utilizado nos *smart cards*.
Um sistema sequencial (SEQ) é semelhante ao HDX, diferindo apenas na forma como se dá a transmissão de energia. A transferência de energia é periodicamente interrompida. Isto permite uma maior poupança energética mas exige um projecto mais cuidado do transponder de modo a que este não perca a sua alimentação durante os períodos de "falha". Normalmente, o transponder possui um condensador que garante a sua alimentação nos períodos de falha. Por outro lado, os tempos de carga, leitura e descarga devem ser cuidadosamente dimensionados (Fig. 9). O sistema EPC utiliza esta técnica de transmissão. O leitor envia *bursts* periódicos de dados /energia para o meio e aguarda por uma resposta do transponder que serve-se das pausas de energia para responder.

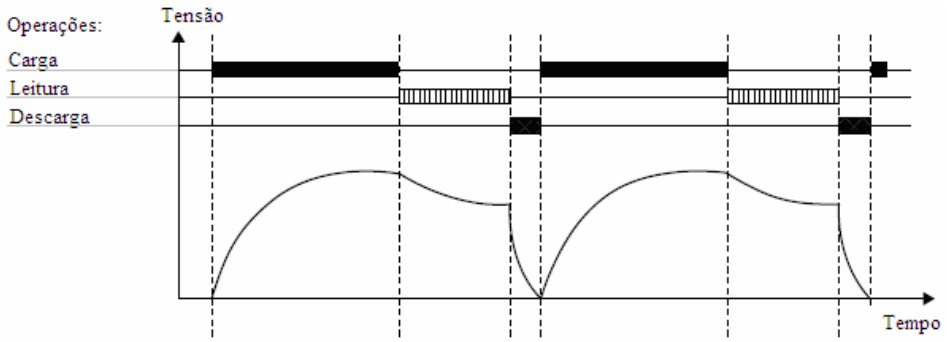


Fig. 9) Fases de operação de um sistema sequencial, retirado de [5]

2.5 – Frequências de operação, potências máximas e alcance

Todos os sistemas rádio estão sujeitos a um conjunto de limitações e imposições de forma a garantir que não haja interferência entre sistemas que coexistem no espaço, tempo ou frequência. No projecto de um sistema rádio há que garantir que este não sofra interferência vinda de outros sistemas nem cause interferência em sistemas adjacentes. Para isso é necessário restringir-se às faixas de frequências disponíveis, não exceder os limites de potência tanto à frequência fundamental como às harmónicas entre outras

limitações. Não fugindo à regra, os sistemas RFID estão também sujeitos a estas restrições. Os sistemas RFID estão alojados na sua grande maioria na banda ISM (Industrial Scientific and Medical). A tabela seguinte [13][14][16] resume a distribuição das faixas de frequências para os sistemas RFID. São também indicadas as potências máximas permitidas para cada faixa, o alcance máximo, algumas aplicações típicas e alguns dos principais fabricantes.

Banda de frequência	**Potência transmitida /Campo H Máximo**	**Alcance Máximo**	**Descrição/Aplicações/Fabricantes**
9 a 135 kHz	72 dBµA/m	Até 20cm	Low Frequency(LF), sistemas indutivos
3.155 a 3.4 MHz	13.5 dBµA/m		Sistemas EAS
6.765 a 6.795MHz	42 dBµA/m		Banda ISM Medium Frequency (MF), acoplamento indutivo
13.55 a 13.567MHz	60 dBµA/m	Até 1m	Medium Frequency (ISM, 13.56 MHz), sistemas indutivos de proximidade utilizados em smart cards contactless (ISSO 14443 A e B, Mifare, LEGIC), cartões de vizinhança smart labels (ISO 15693, Tag-It, I-Code) e ISO 18000-3
26.957 a 27.283 MHz	42 dBµA/m		Medium Frequency, ISM, aplicações especiais, Aplicações Industriais e Hospitalares
433 MHz	10 a 100 mW	Até 100m (activo)	Ultra High Frequency, ISM, backscatter modulation, tags activos
865.6 a 868 MHz	500 mW, Europa		UHF, backscatter modulation, em desenvolvimento
860 a 960 MHz	12 a 37 dBm	Até 10m (EUA) Até 4m (EU)	UHF, ISM, 915 MHz, backscatter modulation, EPC Global, Class 0, Class 1, Gen2, ISO 18000-6A e 6B, EPCGlobal Inc. PHILIPS, Creative Systems, Allien Tecnology
2.4 a 2.483 GHz	4 W, Apenas EUA e Canada	Até 10m	SHF (ISM), backscatter modulation
2.446 a 2.454 GHz	0.5 W em exteriores, 4 W em interiores		SHF - RFID e AVI (Automatic Vehicle Identification)
5.725 a 5.875 GHz	4W EUA, 500mW na Europa		SHF (ISM), backscatter modulation, raramente utilizado para RFID
24,05 a 24,5GHz			Uso futuro

Tabela 2) Distribuição das bandas de frequências para os sistemas RFID

Das bandas de frequências indicadas, destacam-se as bandas LF (125kHz) e HF (13.56MHz) ambas utilizadas em *smart cards contactless* de proximidade e de vizinhança e a banda UHF (860MHz – 960MHz) aplicada nos sistemas EPC (Electronic Product Code).

2.6 – Codificação e Modulação em sistemas RFID

Devido a algumas peculiaridades dos sistemas RFID como a necessidade da transmissão de energia aos *tags* (sistemas passivos), a necessidade de detectar colisões e o facto de os transponders responderem com sinais extremamente fracos (sistemas passivos), a combinação codificação – modulação a utilizar deve ser criteriosamente escolhida. Em muitos casos, é mesmo necessário utilizar uma versão modificada da codificação – modulação "original" que atenda as necessidades próprias da aplicação em causa.
As técnicas de codificação mais utilizados nos sistemas RFID são o código Manchester, o código Miller (e suas variantes modificadas) e o código unipolar retorna zero (RZ). Pelas suas características, estas técnicas de codificação favorecem, por exemplo, a transmissão de energia ou a detecção de colisões. Seguem-se dois exemplos: A norma ISO14443-A utiliza em *downlink* uma versão modificada do código Miller com o intuito de encurtar ao máximo os períodos de "falha" de sinal (energia). Esta codificação baseia-se em pausas curtas a substituir as transições do código Miller original, evitando que o transponder perca a sua alimentação. Esta mesma norma utiliza em *uplink* codificação Manchester que facilita imensamente a detecção de colisões, pois permite distinguir entre três sinalizações diferentes: "1","0" e bit inválido (ocorrência de colisão na interface RF). Este aspecto será detalhado na secção 4.3.1 (Inicialização, anti-colisão e selecção do transponder).
Basicamente, os sistemas RFID servem-se das mesmas técnicas básicas de modulação utilizados nos demais sistemas de comunicação. São elas, a modulação ASK, FSK e PSK.
A modulação ASK – Amplitude Shift Keying é realizada simplesmente pela variação da amplitude da portadora entre dois valores diferentes (A e B) de acordo com o sinal de informação a enviar. Estes dois valores definem o índice de modulação que vem dado por M = (A + B) / (A - B), sendo A o nível alto e B o nível baixo. Em geral, quanto menor é o índice de modulação menor é a probabilidade de erro, sendo que, o caso limite ocorre para M=1 com B=0V (neste caso temos modulação OOK, caso particular do ASK). No entanto, num sistema RFID passivo, há outros aspectos a ter-se em conta nomeadamente a transmissão de energia. Analisando o sistema nesta perspectiva e focando-nos na operação de *downlink*, constata-se que o aumento do índice de modulação é vantajoso para a transferência de energia. Com índices de modulação maiores que 1 eliminam-se os períodos de falha total de sinal (energia) no *tag*. Assim sendo é necessário chegar a um compromisso quando se trata de um sistema RFID. Um exemplo disto é a modulação 10% ASK utilizada pela norma ISO14443-B na operação de *downlink* (Fig. 10). Em nenhum instante, mesmo em *dounlink* (transferência de dados leitor-transponder) há ausência total de sinal/energia no *tag*.

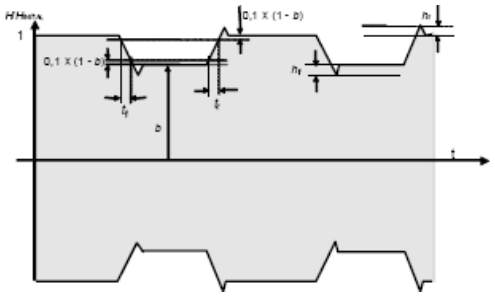


Fig. 10) Modulação 10% ASK utilizada pela norma ISO14443-B (25)

A implementação do modulador e desmodulador ASK é bastante simples quando comparado com o FSK ou PSK. No entanto, este tipo de modulação apresenta uma elevada susceptibilidade ao ruído de amplitude, uma vez que a informação é transportada na amplitude do sinal.
Em FSK – Frequency Shift Keying, a frequência do sinal é simplesmente comutada entre dois valores diferentes representando '0' e '1'. Aqui a informação é transportada na frequência do sinal resultando numa grande imunidade ao ruído de amplitude. No entanto este sistema apresenta uma complexidade acrescida quando comparado com o ASK, visto ser necessário operar com duas frequências distintas.
A modulação PSK – Phase Shift Keying não altera nem a amplitude nem a frequência do sinal. Em vez disto, a comutação da fase do sinal entre dois valores diferentes representa a informação a enviar. O facto de ser uma técnica de amplitude e frequência constante faz dela preferível face às duas anteriores. No entanto apresenta uma grande complexidade de implementação e para frequências muito elevadas (UHF, SHF) começa a tornar-se impraticável, uma vez que, com comprimentos de onda muito baixos é extremamente difícil, quando não impossível, controlar ou detectar a fase do sinal.
A modulação ASK (Phase-Reversal Amplitude-Shift-Keying, PR-ASK; Single-Side Band Amplitude-Shift-Keying, SSB-ASK) é a mais utilizada nos sistemas RFID actuais.
Em geral, quando se escolhe a modulação e codificação para um sistema de comunicação deve-se ter em conta em primeiro lugar a eficiência espectral e a imunidade ao ruído devida a esta escolha. Porém quando se trata de um sistema RFID passivo, há outros aspectos a considerar-se nomeadamente a alimentação do transponder. Esta não pode ser interrompida por uma combinação inapropriada codificação - modulação.

2.7 – Normas e *standards*

A padronização tem influenciado e continuará a influenciar grandemente a forma como as empresas e organizações se posicionam perante o mercado e exploram as possibilidades que este oferece. Os *standards* constituem um forte elo de ligação entre os diversos agentes, não só do mundo tecnológico como de outras áreas de actividade espalhados pelo mundo inteiro, possibilitando compatibilidade e interoperabilidade entre eles. O organismo responsável pelo desenvolvimento de *standards* na área das tecnologias da informação a nível mundial é o Comité Técnico Conjunto ISO/IEC JTC criado pela ISO (International Organization for Standardization) e pela IEC (International Electrotecnical Commission). Apesar de não possuir competências reguladoras, produz normas, procedimentos e regulamentos para um vasto campo de aplicações, fornecendo aos desenvolvedores do

mundo inteiro padrões consistentes e uniformes. Esta secção faz o levantamento de alguns dos principais standards RFID criados até a data. Porém, convém dizer que estão constantemente a surgir novos standards e que os já existentes estão sujeitos a actualização e aperfeiçoamento continuado.
Será aqui feita também uma abordagem mais detalhada ao standard ISO14443-TipoA (utilizado neste projecto) e ao protocolo EPC. A tabela seguinte apresenta as principais normas existentes bem como as frequências de funcionamento e aplicações a que se destinam [5][14][15].

Standard ISO	Designação/Aplicação	Frequências de funcionamento
ISO11784	Identificação animal - Estrutura do código	134.2kHz
ISO11785	Identificação animal – Conceito técnico	134.2kHz
ISO/IEC 15693	Cartões Inteligentes sem contacto de vizinhança (alcance até 1m)	13.56MHz
ISO/IEC 14443	Cartões Inteligentes sem contacto de Proximidade (até 10 cm)	13.56MHz
ISO/IEC 10536	Cartões Inteligentes sem contacto de curta distância	4.9152MHz
ISO/IEC 18001	Tecnologia da Informação - Identificação por Rádio Frequência para gestão de itens	
ISO/IEC 18001 - 1	Parâmetros gerais de comunicação por Interface ar para frequências globalmente aceites	
ISO/IEC 18001 - 2	Parâmetros gerais de comunicação por Interface ar abaixo de 135kHz	>135kHz
ISO/IEC 18001 - 3	Parâmetros gerais de comunicação por Interface ar a 13.56MHz	13.56MHz
ISO/IEC 18001 - 4	Parâmetros gerais de comunicação por Interface ar a 2.45GHz	2.45GHz
ISO/IEC 18001 - 6	Parâmetros gerais de comunicação por Interface ar em 860 – 930MHz	860 – 930MHz
ISO/IEC 18001 - 7	Parâmetros para comunicação activa por Interface ar a 433MHz	433MHz
ISO/IEC TR	Tecnologia da Informação –	

24729-4:2009	RFID para gestão de itens Part 4: Segurança de dados	
ISO/IEC 15961	Tecnologia da Informação – RFID para gestão de itens – Protocolo de dados: Interface de aplicação	
ISO/IEC 15962	Tecnologia da Informação – RFID para gestão de itens – Protocolo de dados: Interface de aplicação: Codificação de dados e funções de memória lógica	
ISO/IEC TR 18046	Métodos de teste de desempenho de dispositivos RFID	
ISO/IEC TR 18047	Tecnologia da Informação – Método de teste conformidade de dispositivos RFID	13.56MHz, 2.45GHz
ISO 1037	Identificação de Contentores (Activo)	850 – 950MHz; 2.4 – 2.5GHz
ISO 18185	RFID para Selo Electrónico (transporte de contentores)	
ISO 23389	Transporte de contentores – RFID Read-Write	
ISO/IEC 19762 – Part3: RFID	Tecnologia da Informação – Técnicas de Identificação Automática e Captura de Dados (AIDC) – Part3: RFID	
ISO/IEC 24730	Tecnologia da Informação – Compatibilidade e Interoperabilidade de Produtos	

Tabela 3) Standards ISO para a tecnologia RFID

Adicionalmente, quando se trata de cartões inteligentes sem contacto, os seguintes *standards* devem ser tidos em conta:
ISO/IEC 7810, Cartões de Identificação – Características Físicas
ISO/IEC 10373-1, Cartões de Identificação – Métodos de Teste – Características Gerais
ISO/IEC 10373-6, Cartões de Identificação – Método de Testes – Cartões de Proximidade
ISO/IEC 15457-1, Cartões de Identificação – Cartões Finos/Flexíveis – Características Gerais
ISO/IEC 15457-3, Cartões de Identificação – Cartões Finos/Flexíveis – Métodos de Teste

2.7.1 – O Standard ISO/IEC 14443 e o protocolo Mifare Standard

Este projecto debruça-se sobre a norma ISO/IEC 14443 implementada pelo protocolo Mifare Standard (excepto a parte 4), pelo que nesta secção pretende-se fazer uma abordagem mais detalhada da mesma.
Os cartões inteligentes sem contacto, conforme os standards internacionais actuais, subdividem-se em três grandes grupos: cartões sem contacto de curta distância segundo o standard ISO/IEC 10536 – *Close Coupled Cards*, cartões sem contacto de proximidade contemplados no standard ISO/IEC 14443 – *Proximity Cards* e cartões sem contacto de vizinhança conforme o standard ISO/IEC 15963 – *Vicinity Cards*. Estes dispositivos são destinados, respectivamente, a operações a distâncias muito curtas (até 1cm), próximas (até 10cm) e longas (até 1m).
O standard ISO/IEC 14443 define os requisitos tecnológicos para a integração da tecnologia RFID com os cartões de identificação (ISO/IEC 7810) e com os cartões finos/flexíveis (ISO/IEC 15457-1). Esta norma não impede o uso de objectos com formatos diversos do standard (cartão rectangular com 81 mm por 49 mm, formato de um cartão multibanco), no entanto desaconselha a integração de outras tecnologias no mesmo cartão [16]. Este *standard* define a comunicação para cartões sem contacto de proximidade e comporta quatro partes:
Parte 1: Características físicas
Parte 2: Potência RF e sinal de interface
Parte 3: Inicialização e anti-colisão
Parte 4: Protocolo de transmissão
A parte 1 descreve as características físicas (formato e dimensões) dos cartões consoante o *standard* internacional (Fig. 11), definindo as dimensões do cartão bem como o posicionamento da antena e do *chip*.

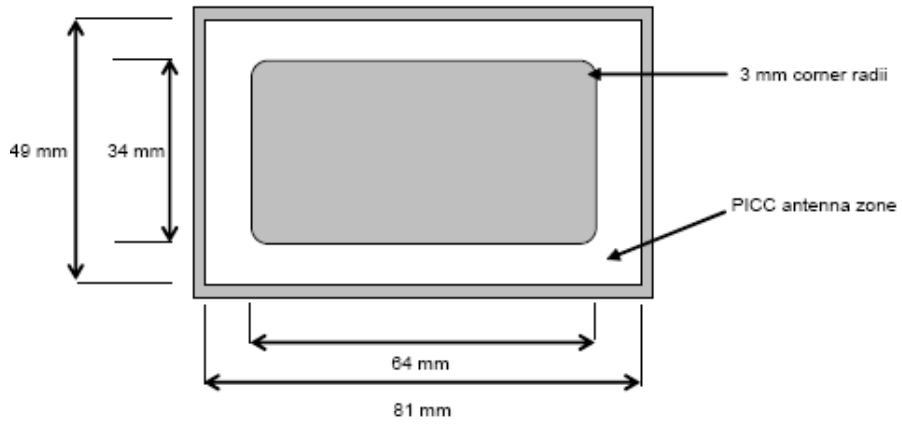


Fig. 11) Características físicas do cartão - ISO14443A&B, retirado de [16]

A parte 2 define as características da comunicação em *downlink* e em *uplink*. Os dados podem ser codificados e modulados de duas formas diferentes, Tipo A (utilizado pela arquitectura Mifare Classic) e Tipo B. A tabela seguinte descreve estas duas variantes [5].

Downlink	Tipo A	Tipo B
Modulação	100% ASK	10% ASK (±2%)
Codificação	Miller modificado	NRZ
Ritmo de transmissão	106 Kbps	106 Kbps
Sincronização	No nível de bit	1 start bit e 1 stop bit
Uplink	**Tipo A**	**Tipo B**
Modulação	Modulação de carga com subportadora a 847 kHz, ASK	Modulação de carga com subportadora a 847 kHz, BPSK
Codificação	Manchester	NRZ
Ritmo de transmissão	106 Kbps	106 Kbps
Sincronização	1 bit sincronização por frame	1 start bit e 1 stop bit por byte

Tabela 4) Especificação da norma ISO14443A&B (Parte 2)

A parte 3 descreve o procedimento de inicialização do cartão e anti-colisão. A anti-colisão permite seleccionar um único cartão de entre os que se encontram no campo do leitor. Após a inicialização e anti-colisão, o cartão ora seleccionado encontra-se no estado activo e está pronto para receber comando de acesso a memória.
A comunicação com os transponders Mifare faz-se de acordo com a parte 3 (Inicialização e anti-colisão) do protocolo ISO14443A. A Fig. 12 apresenta, à direita, o diagrama de estados do transponder segundo a norma ISO14443A e à esquerda a sequência de operações, a ser realizada pelo firmware, para levar um cartão Mifare standard ao estado protocolar. Qualquer transacção de dados é iniciada pelo leitor, através do envio de um comando ao cartão. A unidade digital de controlo do cartão interpreta os comandos recebidos e em função destes responde com dados, código de erro, ACK ou NACK (*not* ACK).
Imediatamente após entrar no campo do leitor (fase POR), o cartão está pronto para receber comandos (estado IDLE). Todas as comunicações são iniciadas com o envio do comando Request All (REQA, WUPA) que acorda todos os cartões no campo, colocando-os no estado READY. Os cartões permanecem neste estado enquanto decorre o processo de anti-colisão (Selecção de um cartão dentre os que estão no campo). O processo de detecção e resolução de colisões será descrito mais adiante. Uma vez terminada a anti-colisão, é seleccionado um cartão através do envio do comando SELECT, cartão este que passa ao estado ACTIVE e devolve o seu UID completo. Para se realizar operações de leitura e escrita na memória do transponder é necessário efectuar a autenticação (Comandos AUTHENTKA ou AUTHENTKB da Mifare), fornecendo a *password* (6 bytes) do sector de memória a que se quer aceder.

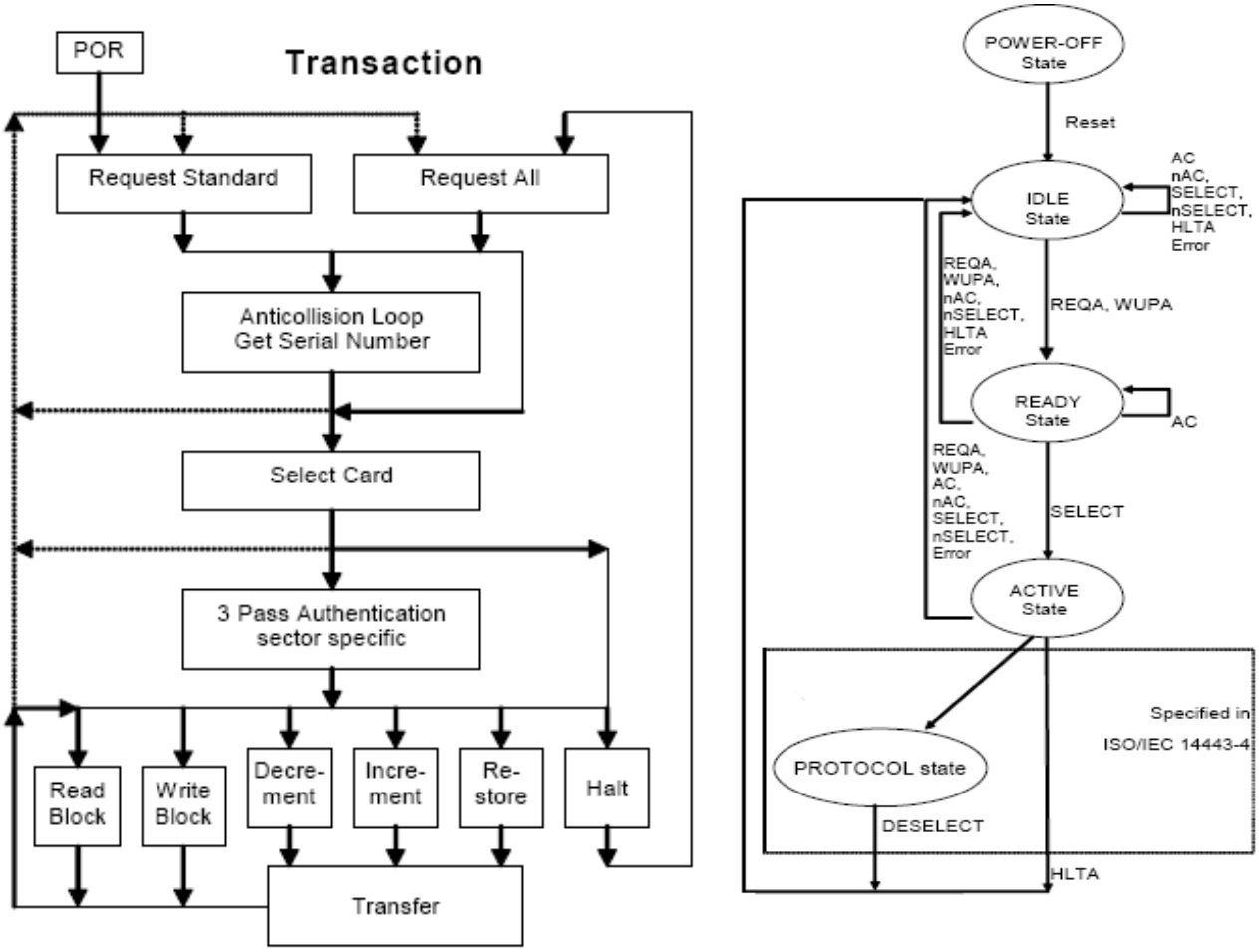


Fig. 12) a) Sequência de Operações; b) Diagrama de estados do transponder segundo ISO14443A-parte 3, retirado de [17]

A parte 4 define o nível protocolar superior. Nesta parte é definida a forma como os comandos devem ser enviados ao cartão. O protocolo Mifare standard não implementa esta parte do standard ISO14443, razão pela qual não se alongará muito mais nesta secção.

2.7.2 – O protocolo EPC Global [18]

Em 1999, foi fundado o Centro de Identificação Automática do MIT (Massachusetts Institute of Technology), o MIT Auto-ID Center, um consórcio de mais de 100 empresas e universidades mundiais (Fig. 1). Em 2003, o MIT Auto-ID Center lançou para o mercado a primeira versão do sistema EPC (Electronic Product Code). Trata-se de um esquema de codificação/identificação criado para substituir o UPC (Universal Product Code - código de barras).

Ainda em Outubro de 2003, a Auto-ID criou a EPCGlobal, que passou a ser a sua sucessora juntamente com a Auto-ID Labs. A EPCGlobal passou a ser responsável pela gestão dos standards e da rede enquanto a Auto-ID Labs ocupou-se da investigação e desenvolvimento da tecnologia EPC. Actualmente o principal objectivo da EPCGlobal é

estabelecer um *standard* RFID global e potenciar o uso da internet para partilha de dados EPC. A ideia é criar uma grande rede RFID onde cada *tag* tenha uma visibilidade alargada e partilhada.
Contando já com diversos standards desenvolvidos, a EPCGlobal tem uma palavra a dizer quando se fala em padronização RFID. Os standards referentes à camada física (Identificação) já desenvolvidos são Class 0, Class 1 e UHF Class 1 Gen 2. Também está a ser desenvolvida pela EPCGlobal uma versão do standard "Gen2" para a banda HF. Convém dizer que a arquitectura EPCGlobal comporta também os níveis protocolares superiores (de aplicação).
O protocolo UHF Classe 1 Geração 2 – Protocolo Interface Ar, também conhecido como "Gen 2" standard define os requisitos físicos e lógicos para sistemas RFID passivos-*backscatter*, *reader talks first*, operando na banda 860MHz a 960MHz.
O sistema EPC tem tido uma grande aceitação a nível mundial, tendo sido adoptado por muitas das grandes cadeias comerciais para catalogação de produtos. Este facto é um bom indicativo de que o RFID está na senda do uso massificado.

2.8 – Fundamentos e princípios de funcionamento

Como já foi referido atrás, os sistemas RFID podem ser agrupados em duas grandes categorias: 1 bit-transponder e sistemas N bits-transponder. Nesta secção serão abordados os fundamentos e princípios de funcionamento por detrás dos sistemas RFID passivos mais utilizados na prática. São eles, os sistemas 1 bit-transponder por efeito não linear (sistemas EAS, anti-roubo), o sistema EPC utilizados para catalogação de produtos e os sistemas por acoplamento magnético utilizados nos *smart cards contactless*. Especial ênfase será dada a estes últimos, que constituem o objecto desta dissertação.

2.8.1 – Sistema EAS - Efeito Não Linear

Os sistemas EAS destinam-se a vigilância electrónica de produtos em estabelecimentos comerciais. Enquadram-se no grupo dos sistemas 1 bit-transpoder e consistem na simples detecção do transponder no raio de cobertura do leitor.
O sistema EAS por efeito não linear explora as características não lineares do diodo. O transponder consiste num simples diodo (dispositivo não linear) que ao ser exposto a radiação (frequência f_A) emitida pelo leitor reflecte múltiplos dessa frequência ($2f_A$, $3f_A$, …), isto é, harmónicas do sinal recebido. O número e a potência das harmónicas dependem do diodo utilizado. A figura seguinte mostra um transponder para um sistema EAS por efeito não linear. Trata-se simplesmente de um diodo acoplado a uma antena de $1/4\lambda$. Por esta razão este tipo de sistemas apresenta um custo muito reduzido, o que o torna ideal para a etiquetagem de grandes quantidades de produtos.

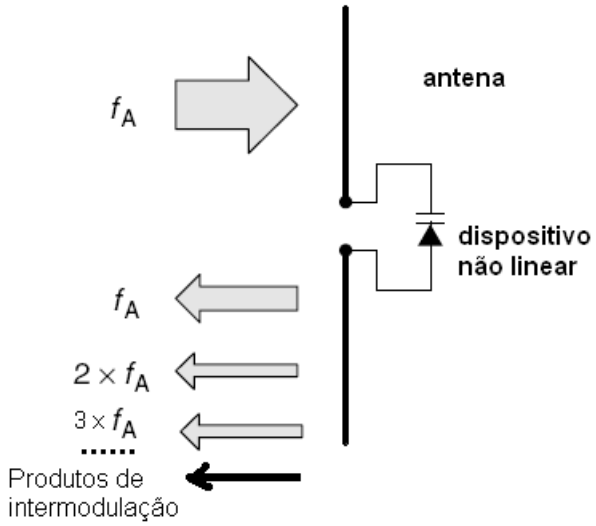


Fig. 13) Transponder EAS - efeito não linear, adaptado de [5]

O princípio de funcionamento é também muito simples. No caso do sistema da figura seguinte, o transmissor gera uma potência a 2.45GHz que, para evitar interferências, é modulada em amplitude por um sinal de 1kHz e radiado para o meio. Quando o transponder entra na zona de interrogação reflecte potência às harmónicas da portadora, 4.9GHz, 7.35GHz, 9.8GHz, …
O receptor usa uma das componentes reflectidas para detectar a presença do transponder na área de cobertura do leitor. Neste caso, temos um sistema de segunda ordem que detecta a segunda harmónica da portadora por meio de um filtro passa banda centrado a 4.90GHz e com uma largura de banda de 1kHz. Tratando-se de um sistema anti-roubo, assim que seja detectado um transponder é imediatamente disparado um alarme.

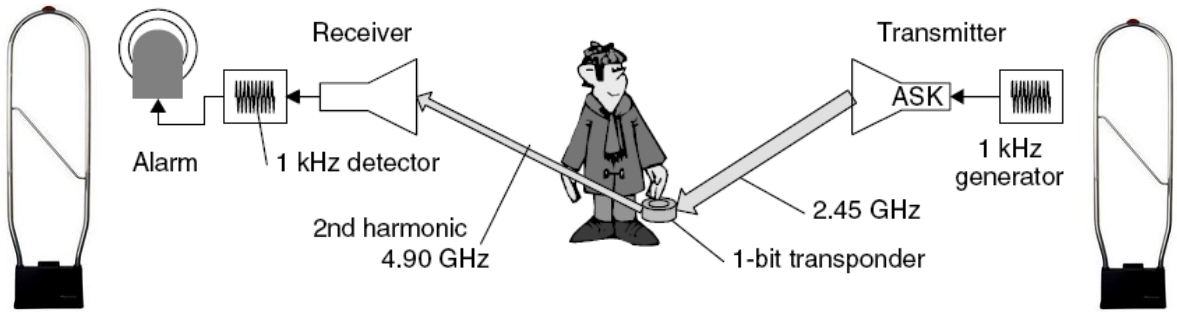


Fig. 14) Sistema EAS - efeito não linear, adaptado de [5]

2.8.2 – Sistema EPC - *Backscatter Modulation*

O standard EPC já foi discutido na secção 2.7.2 "O protocolo EPC Global **".** Nesta secção pretende-se uma descrição do princípio de funcionamento deste sistema. O sistema EPC enquadra-se na categoria dos sistemas N bits-transpoder, passivos, por acoplamento

electromagnético, operando na banda UHF (860MHz – 960MHz). A transmissão de dados do leitor para o transponder é feita por modulação ASK. A alimentação do transponder provém do campo radiado pelo leitor e a transmissão de dados transponder – leitor é realizada por reflexão de potência (*backscatter modulation*). A técnica *backscatter* consiste na modulação do coeficiente de reflexão da antena do tag. O leitor radia potência RF que é recebida pela antena do transponder. Parte desta potência é utilizada para alimentar a electrónica interna do chip e outra parte é reflectida para o meio de acordo com a informação a enviar. Para isso, utiliza-se um transístor de carga (Fig. 15) que é controlado pelos dados binários provenientes do chip. Quando o transístor está OFF (base em aberto), as propriedades da antena (suposta adaptada) não se alteram, não havendo desadaptação da mesma nem reflexão de potência. Isto é interpretado pelo leitor como um nível lógico "0". Quando o transístor está em condução, há uma desadaptação na antena do transponder que provoca reflexão de potência para o meio. Esta reflexão de potência é sentida pelo leitor e percebida como um nível lógico "1".

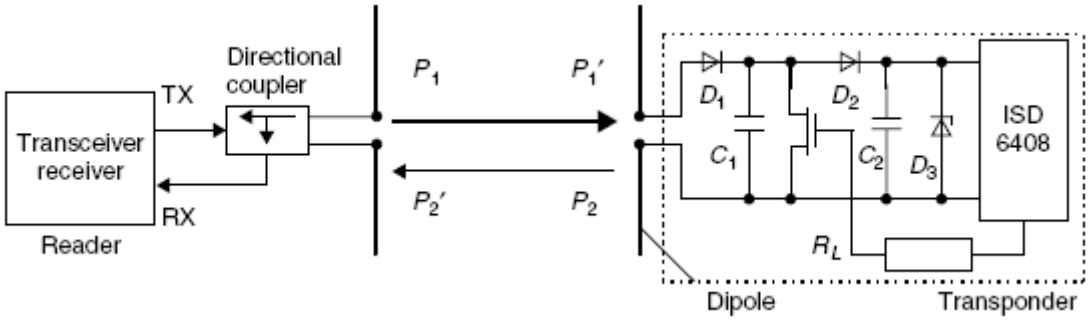


Fig. 15) Sistema EPC - *Backscatter Modulation,* retirado de [5]

O circuito da figura anterior mostra, de forma simplificada, a arquitectura de um sistema passivo com modulação *backscatter*. Os diodos D1, D2 e D3 juntamente com os condensadores C1 e C2 garantem a alimentação regulada do chip. O transístor implementa a modulação do coeficiente de reflexão da antena conforme descrito anteriormente.
Neste sistema, o alcance máximo é determinado pela potência emitida pelo transmissor do leitor, pela sensibilidade do receptor e pelo consumo interno do transponder. Na figura anterior, P1 representa a potência emitida pelo leitor, P1' a potência (fracção de P1) que realmente chega ao transponder após perdas (em espaço livre e por dispersão e multi-percurso), P2 a potência que o transponder é capaz de reenviar para o meio e P2' a fracção de P2 que chega ao leitor após perdas. Algumas considerações importantes a serem feitas são:
1) Para uma dada distância D, a potência P1 deve ser, em todo o caso, superior a P_{perdas} (perdas no meio).
2) A diferença entre P1' e P_{diss} não deve ser nula, isto é, P2 não nulo, sendo P_{diss} a potência consumida pela electrónica interna do transponder.
3) P2' deve ser igual ou superior à sensibilidade admitida pelo receptor do leitor. O balanço de potência ao longo da cadeia de transmissão vem dado por:
$Si = P2' = P1 - 2P_{perdas} - P_{diss}$, sendo Si a sensibilidade do receptor do leitor.

Em geral, os sistemas passivos por acoplamento electromagnético (*Backscatter*) são de longo alcance (até 10 m) e uma vez que operam com comprimentos de ondas curtos permitem a construção de antenas de reduzidas dimensões e elevada eficiência.

2.8.3 – Cartões Inteligentes sem contacto - *Load Modulation*

O *smart card* é uma tecnologia muito difundida actualmente, principalmente em aplicações de pagamento electrónico e em telefones móveis. Um *smart card* consiste num cartão de plástico que incorpora uma memória e eventualmente um microprocessador. Tradicionalmente o cartão possui uma interface de contacto através da qual recebe energia/sincronização e transacciona dados. A capacidade de memória varia de alguns bytes até alguns kbytes, dependendo do fabricante e da aplicação a que se destina.
Actualmente, com o desenvolvimento da tecnologia RFID, os *smart cards* passaram a integrar uma interface de comunicação sem contacto por rádio frequência. Trata-se dos *contactless smart cards*. A Fig. 16 faz a classificação dos *smart cards* de acordo com o tipo de arquitectura e interface de comunicação. Quanto à arquitectura, um *smart card* pode apenas ser de armazenamento (*Memory Card*) ou pode incorporar um CPU que garante maior segurança e autonomia do cartão.

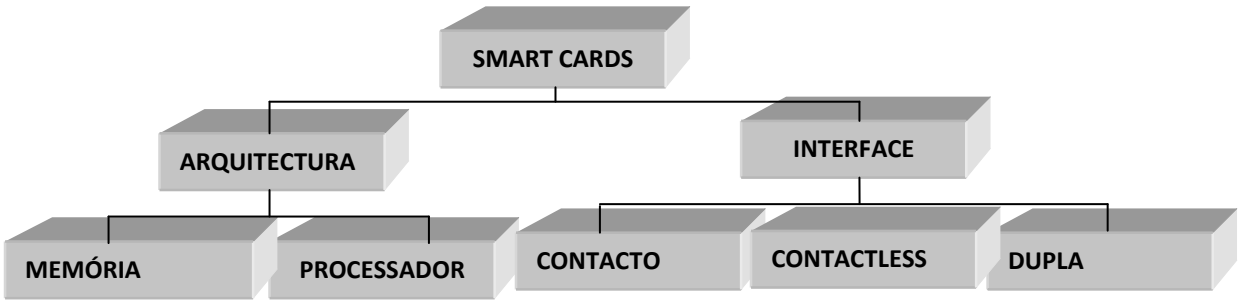


Fig. 16) Classificação dos cartões inteligentes. Arquitectura e interface

O uso da tecnologia RFID nos *smart cards* traz imensas vantagens como a não necessidade de contacto físico nem linha de vista entre o leitor e o cartão, elevados débitos de dados e transacções a longas distâncias (cartões de vizinhança). A figura seguinte classifica os cartões inteligentes de acordo com a interface de comunicação, arquitectura, alcance e frequência de operação [14].
Passar-se-á de seguida a estudar, em maior detalhe, a interface de comunicação RF utilizada nos cartões inteligentes sem contacto, por acoplamento indutivo. Será estudado o princípio de funcionamento, analisando o mecanismo de *uplink* (*Load Modulation*) e de transmissão de energia. Serão igualmente feitas considerações sobre o factor de qualidade e largura de banda da antena e sobre as optimizações necessárias para uma melhor transferência de energia (utilização de circuitos ressonantes).

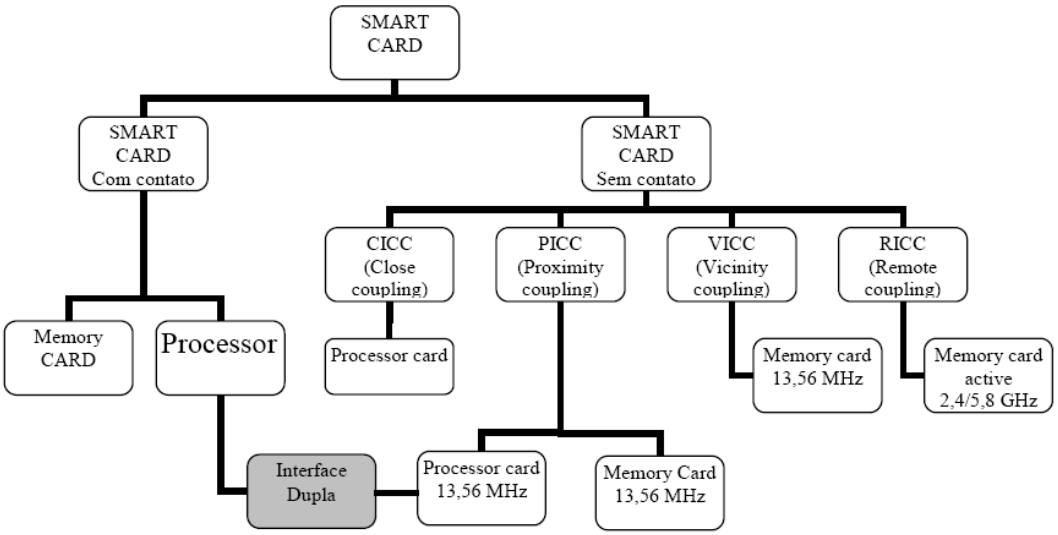


Fig. 17) Classificação dos Cartões Inteligentes. Arquitectura, interface e frequência, retirado de [14]

A figura seguinte mostra a interface RF de um sistema indutivo. O transponder colecta a energia necessária para o seu funcionamento no campo magnético emitido pelo leitor. O envio de dados do leitor para o transponder (*downlink*), segundo a norma ISO14443, é feito por modulação ASK com codificação Miller modificado. Já a operação de *uplink* é realizada por modulação de carga (ASK). Consiste em modular a impedância da bobina do transponder e consequentemente a corrente na bobina do leitor (*Load Modulation*). O *driver* do transístor de carga é feito com a informação binária a enviar ao leitor. Quando a base/gate do transístor de carga está OFF (em aberto), não há alterações no secundário (bobina do transponder) nem na corrente do primário (bobina do leitor). Isto é percebido pelo leitor como um nível lógico "0". Quando a gate está ON, há um curto-circuito no secundário provocando um aumento de corrente no primário. Este aumento de corrente é sentido pelo leitor e percebido como um nível lógico "1".

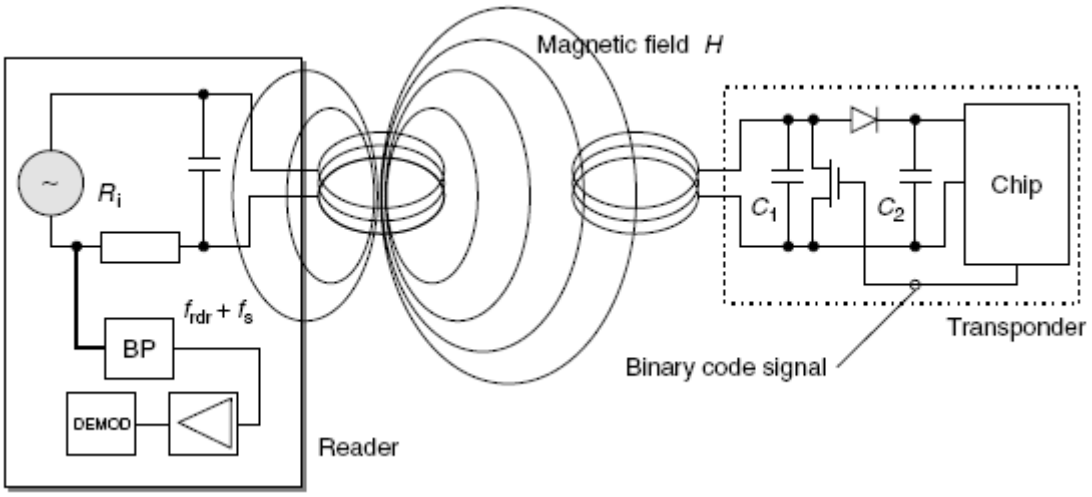


Fig. 18) Sistema indutivo - Backscatter modulation, retirado de [5]

Do ponto de vista da transmissão de energia, um sistema RFID com acoplamento indutivo pode ser visto como um transformador com núcleo de ar (Fig. 19) em que a bobina (antena) do leitor equipara o primário com uma indutância L1 e a bobina do transponder o secundário com uma indutância L2. O primário (antena do leitor) e o secundário (antena do transponder) estão acoplados por uma indutância mútua M (factor de acoplamento magnético $K = \frac{M}{\sqrt{L1.L2}}$).

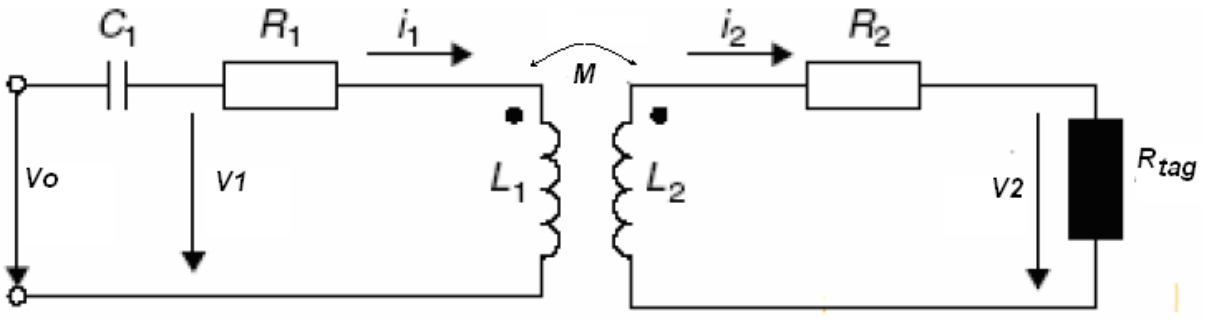


Fig. 19) Circuito magnético equivalente

A figura anterior mostra o circuito magnético equivalente para um sistema RFID indutivo (neste caso a funcionar a 13.56MHz). *L1* e *L2* representam respectivamente a indutância da bobina do leitor e do transponder, M é a indutância mutua entre as duas bobinas, *R1* e *R2* correspondem as perdas nos dois enrolamentos e finalmente R_{tag} representa o consumo DC interno do transponder. A corrente variável *i1* (que para simplificar vai passar a ser referido apenas como *i1*) que flui sobre L1 provoca um fluxo variante no tempo que induz em *L2* uma tensão dada por $M\frac{di1}{dt}$. Por sua vez a corrente *i2* (que para simplificar vai passar a ser referido apenas como *i2*) gera na malha secundária uma força electromotriz devido a *L2* dada por $L2\frac{di2}{dt}$ e uma outra devido a *R2*. Vem então a seguinte equação [5]:

$$V_2 = M\frac{di1}{dt} - L2\frac{di2}{dt} - i2.R2 \qquad \textbf{(Eq.1)}$$

Passando para o domínio Laplaciano vem V2(S) = M.I1(S).S – L2.I2(S).S – I2(S).R2. Fazendo I2(S) = V2(S)/R_L e S = *jw* e, V_2 vem na frequência dado por:

$$V_2 = \frac{jwM.i1}{1+\frac{jwL2+R2}{RL}} \qquad \textbf{(Eq.2)}$$

Ressonância, factor de qualidade Q e largura de banda B

A tensão V_2 induzida na bobina do transponder constitui a fonte de alimentação do chip. Assim sendo, a "eficiência" do circuito da figura anterior deverá ser optimizada de modo a conseguir-se uma boa transferência de energia do leitor para o transponder. Por outro lado é preciso ter em conta a largura de banda mínima necessária para a transferência de dados.
A maximização da transmissão de energia é conseguida à custa da utilização de circuitos ressonantes em ambas as antenas.

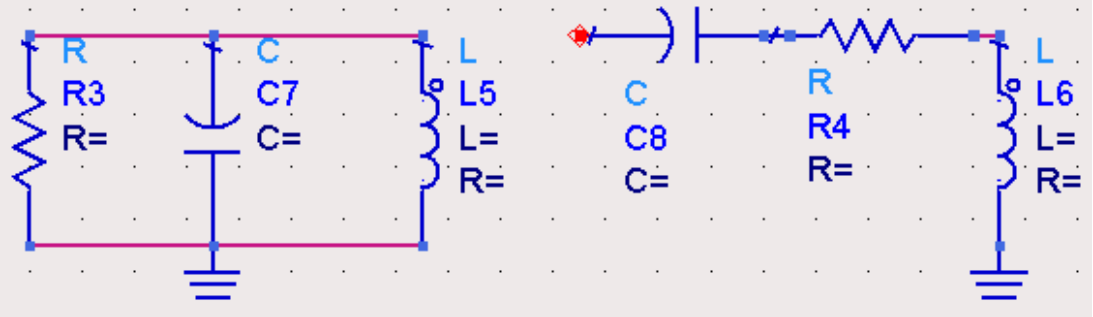


Fig. 20) Esquerda: RLC paralelo. Direita: RLC Série

Ressonância

A ressonância dá-se em circuitos eléctricos que possuem pelo menos dois armazéns de energia (um indutivo e outro capacitivo) responsáveis pela oscilação da energia armazenada de uma forma para outra. Dependendo do valor dos componentes do circuito, este terá uma frequência própria de ressonância para a qual ocorre um pico de amplitude de tensão ou corrente (conforme se esteja na presença de um circuito série ou paralelo). No caso do circuito RLC, uma vez atingida a condição de ressonância, as reactâncias capacitiva e indutiva cancelam-se mutuamente. Deste modo a impedância equivalente do circuito passa a ser puramente resistiva.
Na secção seguinte é feita uma breve análise do comportamento na frequência do RLC série e paralelo. É analisada a impedância, tensão e corrente, coeficiente de reflexão e factor de qualidade.

Circuito ressonante paralelo

O circuito ressonante RLC paralelo (Fig.19), na sua forma natural, com entrada em corrente e saída em tensão, é um filtro centrado na frequência de ressonância f_o e com uma largura de banda B, cuja função de transferência coincide com a impedância equivalente do circuito. A razão entre a frequência de ressonância e a largura de banda corresponde ao factor de qualidade *Q* do filtro. Estes três parâmetros serão ajustados de modo a conseguir-se um óptimo desempenho do circuito. A função de transferência deste filtro vem dada na frequência pela seguinte equação [28]:

$$H(jw) = \frac{V(jw)}{I(jw)} = Zeq(jw) = \frac{1}{jwC + \frac{1}{jwL} + 1/R} \qquad \textbf{(Eq.3)}$$

A frequência de ressonância é aquela para a qual a entrada e a saída do circuito estão em fase e é dada por:

$$Wo = \frac{1}{\sqrt{L.C}} \Rightarrow fo = \frac{1}{2\pi\sqrt{L.C}} \qquad \textbf{(Eq.4)}$$

B define a banda passante do filtro na qual o sinal sofre uma atenuação igual ou inferior a 3dB e é dado por:

$$B = f2 - f1 = \frac{1}{2\pi RC} \quad \textbf{(Eq.5)}$$

O factor de qualidade do filtro, *Q* é uma medida da selectividade da frequência de interesse e corresponde à razão entre a energia armazenada no circuito num ciclo e a energia dissipada neste mesmo ciclo. Vem dado por:

$$Q = \frac{fo}{B} = \frac{RC}{\sqrt{L.C}} \quad \textbf{(Eq.6)}$$

É fácil de se constatar que a impedância equivalente do circuito é:

$$Zeq(jw) = \frac{1}{jwC + \frac{1}{jwL} + 1/R} \quad \textbf{(Eq.7)}$$

Zeq(j*w*) atinge um máximo para $w=w_o$. Consequentemente este circuito apresenta um máximo de tensão à frequência de ressonância. Desprezam-se aqui as perdas intrínsecas da bobina.

Circuito ressonante série

Uma análise idêntica é feita ao circuito RLC série (Fig.19), considerando desta vez entrada em tensão e saída em corrente [28]:

$$H(jw) = \frac{I(jw)}{V(jw)} = Yeq(jw) = \frac{1}{R + j(wL - \frac{1}{wC})} \quad \textbf{(Eq.8)}$$

$$Wo = \frac{1}{\sqrt{L.C}} \Rightarrow fo = \frac{1}{2\pi\sqrt{L.C}} \quad \textbf{(Eq.9)}$$

$$B = f2 - f1 = \frac{R}{2\pi.L} \quad (Hz) \quad \textbf{(Eq.10)}$$

$$Q = \frac{fo}{B} = \frac{\sqrt{L}}{R\sqrt{C}} = \frac{woL}{R} = \frac{2\pi foL}{R} \quad \textbf{(Eq.11)}$$

O correcto dimensionamento do factor de qualidade *Q* é preponderante para um bom desempenho do sistema. *Q* deve ser uma solução de compromisso. Um *Q* muito baixo, degrada a transferência de energia leitor transponder, pois teremos um circuito ressonante pouco selectivo à frequência de operação. Por outro lado, deve-se ter em conta a largura de banda necessária para a transmissão de dados em ambos os sentidos, o que impõe uma largura de banda mínima B_{min} e consequentemente um factor de qualidade máximo Q_{max}. Para que a informação seja recuperada, a antena do receptor deverá ter uma largura de banda correspondente a pelo menos o dobro do ritmo de transmissão de dados (supondo codificação NRZ não formatada, modulação ASK).

$$Zeq(jw) = R + \frac{1}{jwC} + jwL = R + j(wL - \frac{1}{wC}) \qquad \textbf{(Eq.12)}$$

Da equação anterior constata-se que para a frequência de ressonância, o circuito apresenta um mínimo de impedância (puramente real) de valor R, o que traduz-se num máximo de corrente a esta mesma frequência. Esta corrente máxima pode ser controlada variando o valor de *R*.
As figuras seguintes representam a variação da impedância e do coeficiente de reflexão S_{11} com a frequência. f_o representa a 1ª ressonância[1] do circuito.

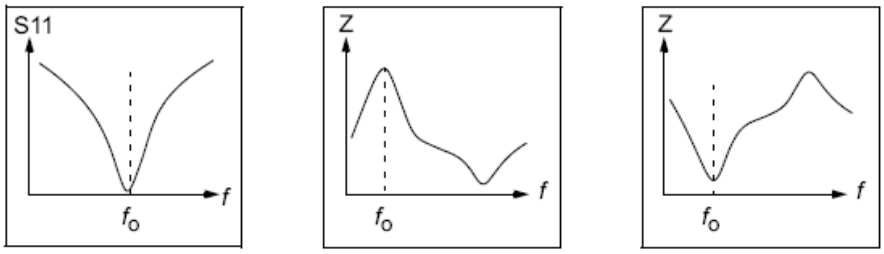


Fig. 21) a) Coeficiente de Reflexão, b) Impedância circuito Paralelo, c) Impedância circuito Série

Em 21-a, o mínimo observado representa um mínimo de reflexão na frequência de ressonância, ou seja, o circuito absorve a máxima potencia que lhe é entregue a esta frequência enquanto rejeita (reflecte) potência nas restantes frequências. Do ponto de vista da adaptação, temos uma adaptação máxima à frequência de ressonância.
Em 21-b, a curva de impedância apresenta um máximo à frequência de ressonância o que se traduz num pico de tensão. Este circuito será, portanto, ideal para maximizar a eficiência da antena do transponder, uma vez que o transponder é alimentado pela tensão colectada na sua antena. Assim sendo, se o circuito da antena do transponder for um circuito ressonante paralelo ajustado à frequência de ressonância (neste caso 13.56MHz) terá o seu desempenho melhorado, permitindo melhorar o alcance e eficiência energética. O circuito ressonante no transponder é conseguido com a introdução de um condensador em paralelo com a antena (bobina). Nesta dissertação incide-se no projecto do leitor, assume-se que os transponders estão devidamente adaptados, pelo que o estudo da adaptação da antena apenas será feito para o leitor.
Em 21-c, pode-se observar um mínimo de impedância à frequência de ressonância, o que leva a um pico de corrente a esta mesma frequência. O circuito RLC série é usado no leitor a fim de conseguir uma maior corrente (à frequência de ressonância) na bobina da antena e consequentemente um maior fluxo magnético e maior distância de leitura.
Da análise anterior conclui-se que a eficiência do sistema emissor-receptor de energia (leitor-transponder) pode ser maximizado se o emissor for adaptado com um circuito ressonante série, o receptor com um ressoante paralelo e ambos forem ajustados à mesma frequência de ressonância. Desta forma consegue-se um canal sintonizado por onde se dá a transferência de energia. Numa primeira análise, bastaria adaptar separadamente o leitor e o transponder para se conseguir tal feito. No entanto, numa análise mais cuidada há que ter em conta, entre outros aspectos, efeito de carga do transponder sobre o leitor, que resulta

[1] O circuito possui uma segunda ressonância a uma frequência mais elevada

da impedância equivalente do transponder vista no primário (antena do leitor) e a interferência entre transponders. Este aspecto será avaliado experimentalmente na secção 5.2 (Estudo e caracterização da bobina da antena)

Capítulo 3 – Projecto do leitor/gravador RFID (13.56MHz)

3.1 – Considerações gerais

Antes de se avançar para o projecto do hardware, vão ser feitas algumas considerações acerca do mesmo: O *core* do leitor será o transceiver RFID MFRC531 da NXP, que suporta a norma ISO14443-A (*Identification cards - Contactless integrated circuit(s) cards – Proximity cards*) e a ISO14443-B (*Proximity Contactless Identification Cards*). A unidade de processamento a utilizar será um ATmega16 (da Atmel), conectado ao transceiver por SPI. Adicionalmente haverá uma linha de interrupção externa entre o transceiver e o MCU. Numa primeira fase (placa provisória) a comunicação PC-MCU é efectuada pelo protocolo RS232 recorrendo a um controlador RS232 (MAX232), sendo que, posteriormente será substituído pelo protocolo USB (versão final da placa). Depois de um estudo do comportamento de antenas (bobinas) de tamanhos e formatos diferentes em fio e em PCB, concluiu-se que a melhor opção seria uma bobina de três espiras em PCB (formato rectangular).

3.2 – Diagrama de blocos

A Fig. 22 mostra o diagrama de blocos do sistema a desenvolver. A terminologia *Front-End* aqui utilizada é um tanto quanto rebuscada. Na realidade não se utilizou amplificador de potência nem amplificador de baixo ruído externo. O bloco *Front-End* representa o conjunto da antena (bobina, circuito ressonante, adaptação, circuito de recepção). Especial cuidado foi tido com a filtragem da alimentação. O bloco TX FILTER tem o papel idêntico ao de um RF CHOKE, operando como um DC *Feed* e impedindo que a alta frequência de potência (13.56MHz) perturbe a alimentação DC. Também a alimentação da parte digital e analógica do transceiver foi filtrada com o filtro A/D FILTER.
O consumo de energia do leitor pode ser directamente controlado a partir do MCU. Isto é conseguido colocando o transceiver em modo de baixo consumo quando este não esteja a ser utilizado ou desligando o receptor/transmissor. O *reset* do MCU é simultâneo à fase POWER-ON do leitor, enquanto o *reset* do transceiver é da responsabilidade do próprio MCU.
O MCU envia comandos ao transceiver (via PSI) que sinaliza a execução do comando ou a ocorrência de erros através da linha de interrupção IRQ. Finalmente, o servidor de aplicações (PC) comunica-se com o MCU através da interface RS232/USB.

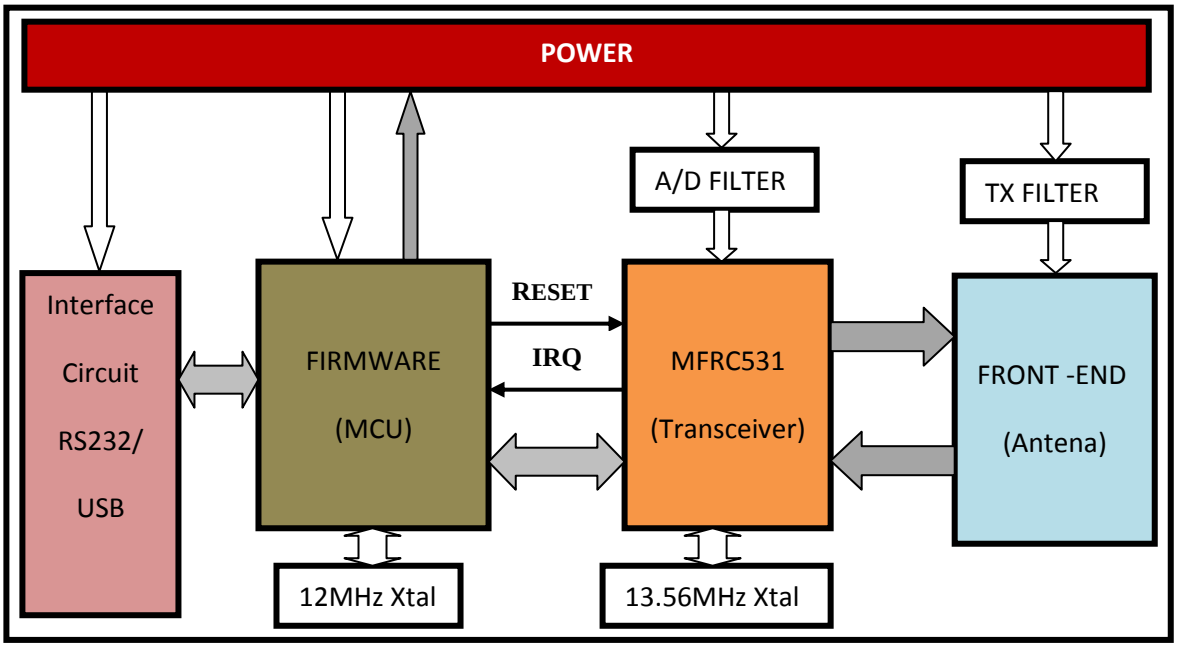


Fig. 22) Diagrama de blocos do leitor

3.3 – Descrição do CPU, do transceiver e do transponder utilizado

O microcontrolador utilizado é um ATMega16 da Atmel. Trata-se de um micro de 8 bits, CMOS de baixo consumo baseado na arquitectura AVR RISC. Conta com 512 Bytes de memória EEPROM, 16 KBytes de memória de programa (Flash) e 1 KByte de memória de dados (SRAM). Suporta comunicação Serial USART e SPI [19]. Constitui a unidade de processamento *on-board* do sistema responsável pelo *firmware*.
O *core* do leitor é o transceiver RFID HF da NXP, o MFRC531 (Fig.23). Este transceiver faz parte da nova família de leitores RFID altamente integrados para comunicação sem contacto na banda dos 13.56MHz. Esta família suporta todos os protocolos para a tecnologia passiva de cartões sem contacto de proximidade. Para além do chip utilizado neste projecto, fazem parte desta família os transceivers MFRC500, MFRC530, e SLRC400.
O MFRC531 combina todas as funcionalidades básicas de um leitor RFID HF, integrando um transmissor, um receptor, modulador, desmodulador e banda base num único chip. Inclui todos os blocos RF para interrogar e receber dados do transponder: VCO (*Voltage Controled Oscilator*), amplificador de ganho variável, detector de envolvente, receptor/desmodulador em fase e quadratura (IQ) e um transmissor preparado para ser ligado a uma antena projectada para distâncias de até 100 mm.
Este chip, suporta todas as camadas do standard ISO14442A e B incluindo o mecanismo de anti-colisão e admite comunicação usando os ritmos mais elevados da arquitectura Mifare[2] (424 Kbps e 848 Kbps).

2 Apesar de o chip suportar estes ritmos, utiliza-se neste projecto apenas o ritmo mais baixo (106Kbps) que é o utilizado pelos cartões Mifare Standard 1K e 4K

Adicionalmente o MFRC531 incorpora funcionalidades de banda base configuráveis que permitem, por exemplo, comutar entre diferentes ritmos de transmissão de dados ou entre diferentes tipos de modulação/codificação de modo a compatibilizar-se com transponders tipo A ou tipo B.
O transceiver conta ainda com diversos mecanismos de detecção e correcção de erros e de integridade e segurança de dados. São eles, a geração e verificação de paridade simples, a geração e verificação de checksum (CRC), o BCC, a encriptação de dados e a autenticação aquando de operações na memória dos transponders. A encriptação de dados é feita por um algoritmo proprietário da NXP denominado CRYPO1. Este algoritmo é até hoje mantido secreto pela NXP, não sendo divulgada a chave pública [20].
Finalmente, o acesso ao banco de registos internos do chip pode ser feito tanto por interface paralela de 8 fios como por interface série, SPI. Neste projecto opta-se pela interface SPI por ser a mais "compacta".

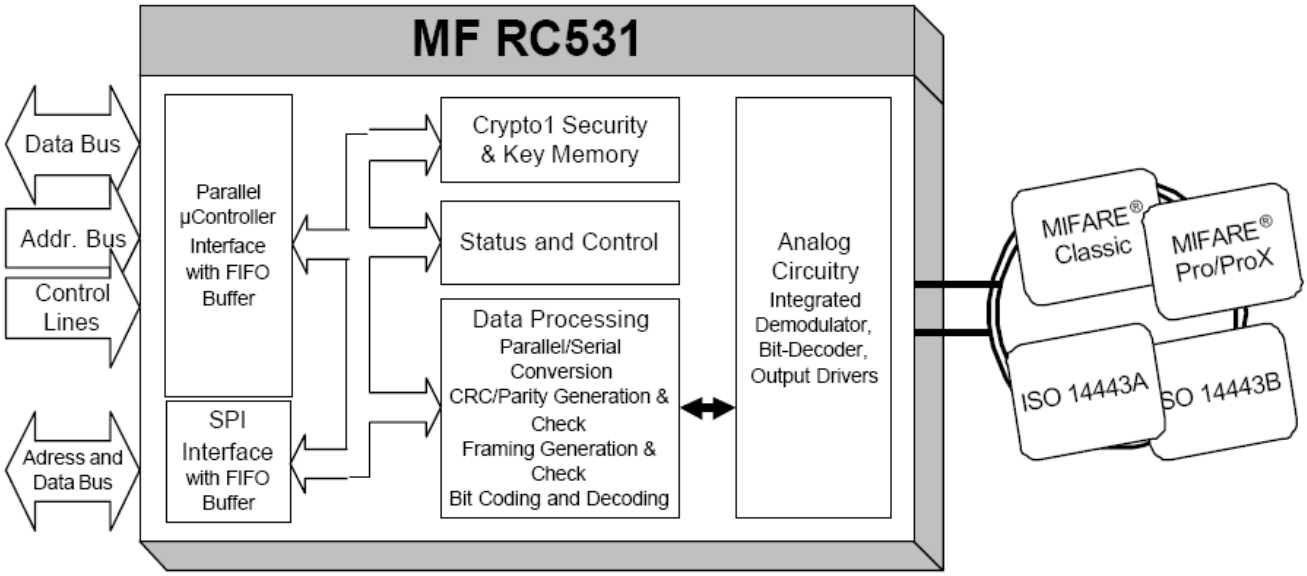


Fig. 23) Diagrama de blocos do transceiver, retirado de [21]

Arquitectura dos transponders Mifare Standard [22][23]

Os transpoders escolhidos para este projecto são os da família Mifare Standard cujo fabricante é a NXP Semiconductors (mesmo fabricante do transceiver utilizado). Trata-se de uma família de *smart cards contactless* compatíveis com as partes 1, 2 e 3 do standard ISO14443A. Pretende-se fazer aqui uma breve descrição a arquitectura dos cartões Mifare Standard do ponto de vista do hardware e da organização lógica da memória. A figura seguinte mostra o diagrama de blocos de um *smart card contactless* da Mifare.

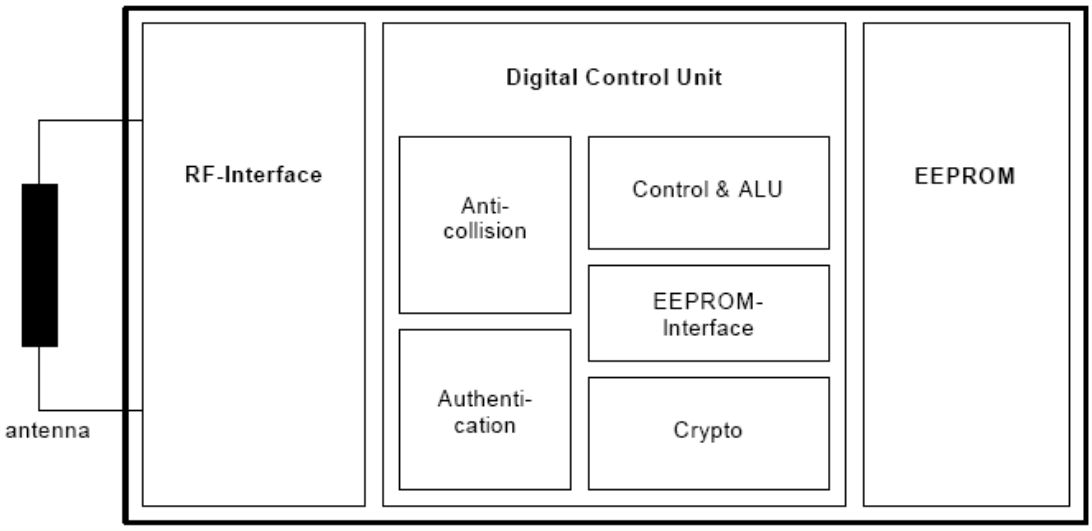


Fig. 24) Tag Mifare - Diagrama de blocos, retirado de [23]

Os *chips* MF1ICS50 e MF1ICS70 consistem em, respectivamente 1KByte e 4KByte de memória EEPROM, uma interface RF e uma unidade digital de controlo. A transferência de energia, temporização (*clock*) e dados é feita através de uma antena (bobina) directamente conectada ao chip. A interface RF é constituída por:

- Modulador/Desmodulador
- Rectificador e regulador de tensão para alimentação do chip
- Extractor de relógio que recupera a componente fundamental a 13.56MHz
- Circuito *Power On Reset* que tem como função acordar o chip quando este entra no campo do leitor.

A unidade digital de controlo incorpora funcionalidades de anti-colisão, permitindo que vários cartões sejam servidos "simultaneamente" pelo mesmo leitor, autenticação nas operações de acesso à memória do chip e encriptação de dados nas transacções com o leitor.
Uma vez o cartão seleccionado e activado por um leitor autorizado, podem ser realizadas as seguintes operações de acesso a memória: leitura/escrita de blocos, incremento/decremento de blocos formatados como VALUE [3]. Estas operações são realizadas respectivamente pelos comandos WRITE, READ, INCREMENT e DECREMENT.
À parte a capacidade da EEPROM, a organização lógica da memória dos cartões de 1KByte e de 4KByte é em tudo idêntica. A memória está dividida em blocos de 16 bytes cada. Estes blocos estão agrupados em sectores. Esta estratégia permite ter no mesmo cartão múltiplas aplicações de múltiplos servidores, uma vez que, cada sector possui uma *password*.

[3] Na arquitectura Mifare, há a possibilidade de formatar blocos de memória como "valor". Estes blocos possuem um formato especial permitindo apenas o incremento ou decremento do seu valor. Esta aplicação pode ser útil, por exemplo, para a implementação de um sistema de crédito/débito.

O cartão 1KByte possui 16 sectores de 4 blocos cada. Já o cartão 4KByte consiste em 32 sectores de 4 blocos e 8 sectores de 16 blocos cada. Cada sector de dados possui um bloco de cabeçalho (*sector Trailer*). O diagrama lógico da memória é mostrado na (Fig. 25).
O bloco 0 do sector 0 é um bloco especial apenas de leitura. Contém o UID do cartão e dados do fabricante.
O *trailer* de cada sector contém as chaves secretas de acesso A e B usadas para autenticação e as condições de acesso aos blocos do sector (Fig. 26). As condições de acesso definem as permissões de leitura/escrita em cada bloco de dados do sector.
O "*sector trailer*" possui condições de acesso especiais, a chave A nunca é legível, enquanto, a chave B pode ser configurada para o ser ou não. A organização do *sector trailer* é mostrada na Fig. 26.

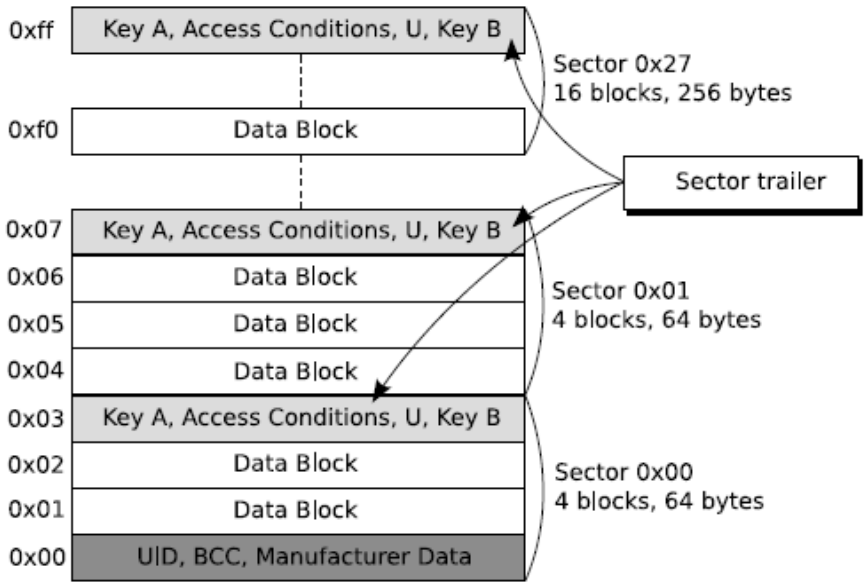


Fig. 25) Organização lógica da memória, retirado de [20]

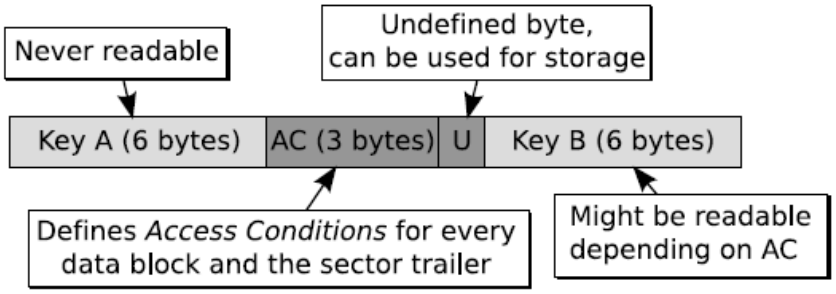


Fig. 26) *Sector Trailer*

3.4 – Adaptação da antena

Na realidade, a antena utilizada nos sistemas de proximidade com acoplamento indutivo não é uma antena no sentido convencional. A componente eléctrica do campo electromagnético (campo E) não é utilizada para comunicação neste tipo de sistemas,

apenas a componente magnética (campo B) é utilizada. Deste modo, a antena deste tipo de sistemas é uma simples bobina.
O campo magnético é gerado pelo leitor, através de uma corrente na bobina (antena). Nesta e nas secções seguintes será dimensionado o bloco da antena (Fig.27) tendo em atenção as limitações do transceiver e as especificações impostas pelo standard ISO 14443.

O bloco da antena é composto pela bobina da antena e circuito ressonante, circuito de adaptação e circuito receptor. As funcionalidades deste bloco podem ser divididas em:

1. Transmissão de energia: O campo magnético radiado deve ser maximizado de acordo com os limites impostos, especialmente limitações de corrente à saída de TX1 e TX2 (I_{TXMAX}=150mA) e da potência emitida pelas harmónicas (até 1GHz);
2. Transmissão de dados: Especificações (tempos de subida/descida e *overshoot*) do sinal 100% ASK devem ser cumpridas para que os transponders possam receber correctamente o sinal;
3. Recepção de dados: a resposta do transponder deve ser entregue ao circuito de acordo com as limitações do MFRC531 (1.5Vpp < V_{RX}< 3Vpp);

A Fig.27 mostra o circuito completo da antena. R_{ext} + R_{coil}, C1 e La constituem o circuito ressonante estudado na secção "Circuito Ressonante série". O circuito constituído por C0 e L0 é um adaptador elevador de impedâncias cuja função é adaptar a impedância da antena (ressonante) à impedância que deve ser vista por TX1/TX2. Finalmente, o circuito de recepção acondiciona o sinal de entrada do receptor. Este sinal deverá ser referenciado a uma tensão de referência interna do transceiver (VMID) e a sua amplitude deverá estar entre 1.5Vpp-3Vpp.

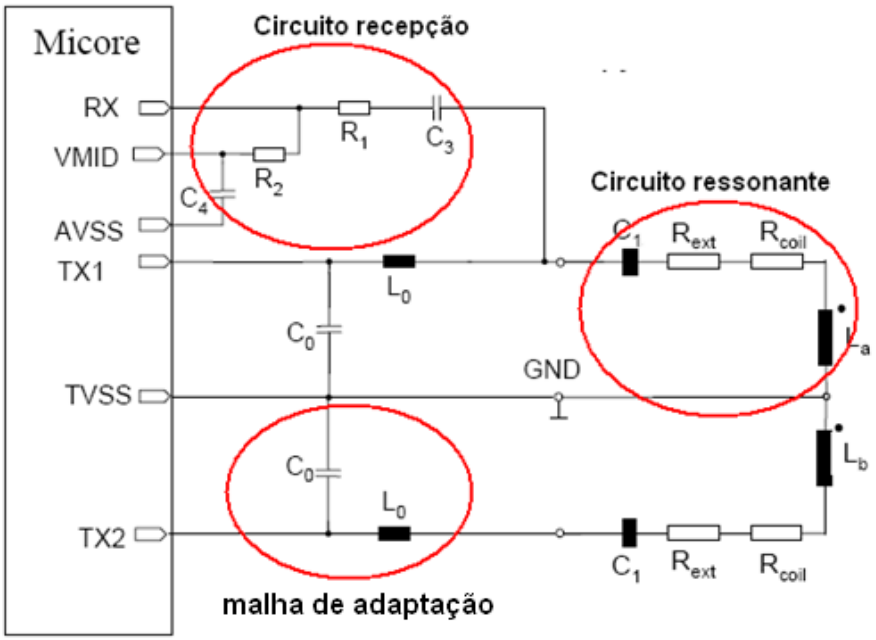


Fig. 27) Antena do leitor

3.4.1 – Frequência de funcionamento e Largura de banda mínima

O circuito será dimensionado para a frequência de ressonância de 13.56MHz. O standard ISO14443-Parte 2 (potência RF e sinal de interface) define para o Tipo A, um ritmo de transmissão de dados (em ambos os sentidos) $\mathrm{RTx} = \frac{\mathrm{fc}}{128} = 106\mathrm{Kbps}$ (ritmo usado pelos transponders Mifare standard 1KByte e 4KByte de memória). Consequentemente $Q_{max} = \frac{\mathrm{fo}}{\mathrm{Bmin}} = 64$. Valores superiores a este poderão levar à perda de informação, uma vez que, o filtro não terá largura de banda suficiente.

3.4.2 – Factor de qualidade Q

O fabricante do transceiver recomenda, para o circuito ressonante da antena, um factor de qualidade de Q=30. Este valor cumpre com a especificação imposta pela largura de banda mínima e garante um bom funcionamento do circuito ressonante.

3.4.3 – Adaptação e Optimização recorrendo ao ADS

Para o dimensionamento e adaptação do circuito da antena, três especificações devem ser tidas em conta:

1- Valor minímo da impedância de carga (Z_{mim}= 20 Ω) vista por TX1 e TX2 (Fig. 28) recomendada pelo fabricante. Esta impedância não deverá fazer exceder o valor máximo de corrente, Imax

2- Frequência de operação/ressonância da antena (fc=13.56MHz)

3- Factor de qualidade (largura de banda) do circuito ressonante da antena
Na figura seguinte, R_{coil} é a resistência natural da bobina e R_{ext} é uma resistência adicional que tem como finalidade ajustar o factor de qualidade do circuito. A indutância da bobina, L_{coil} define juntamente com R o factor de qualidade do filtro. O condensador C1 juntamente com L_{coil}, definido anteriormente, sintonizam o filtro definindo a sua frequência de operação/ressonância. A impedância equivalente do circuito ressonante à frequência de ressonância, Z_{eq} (Fig. 28) é puramente real de valor $R = R_{ext} + R_{coil}$.

O circuito é simétrico em relação a TVSS (na arquitectura Mifare TX1 entrega a portadora modulada e TX2 a portadora modulada invertida). Assim sendo duas considerações de simetria vão ser aplicadas (cada meia bobina da antena apresenta uma resistência de perdas $R_{coil} = R_L/2$ e uma indutância $L_{coil} = L/2$), permitido que a análise seja feita apenas à metade superior, sendo igualmente aplicável à inferior.

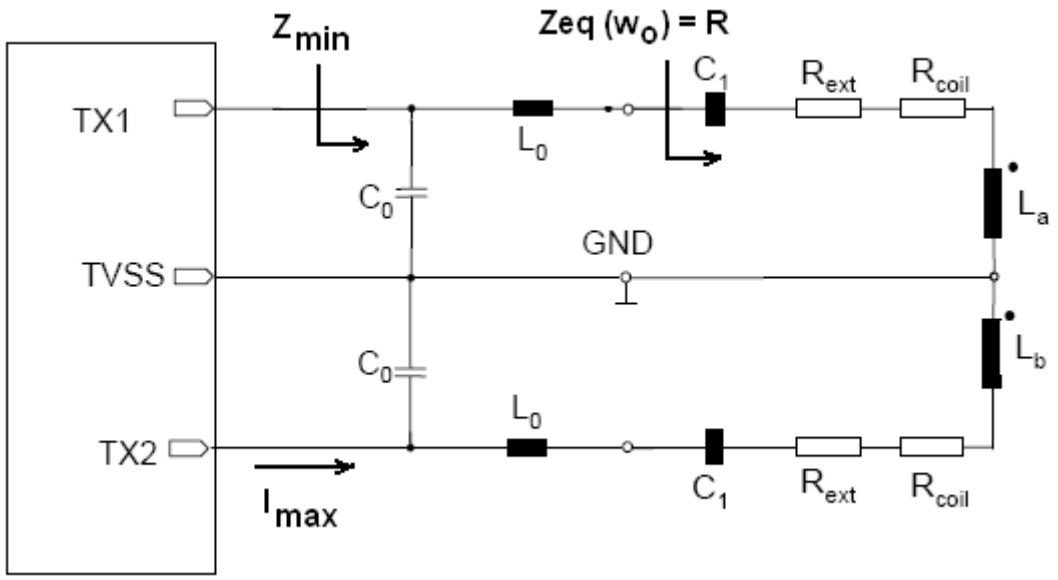


Fig. 28) Adaptação da antena com malha em L

A adaptação da antena vai passar pela determinação de uma primeira aproximação para os componentes e posterior optimização (recorrendo à simulação em ADS) de modo a cumprir as especificações impostas.
Dado o valor de Q e L_{coil} (medido), começa-se por calcular a resistência total do circuito ressonante que garante Q. $R_{Total} = R_{ext} + R_{coil}$ vem dado por:

$$Q = \frac{w.L_{coil}}{R_{Total}} \quad \Rightarrow \quad R_{Total} = \frac{w.L_{coil}}{Q} \qquad \textbf{(Eq.13)}$$

O valor da resistência a acrescentar em série com a resistência natural da bobina será então:

$$R_{ext} = R_{Total} - R_{coil}\,,\ com\ \ R_{coil}\ medido \qquad \textbf{(Eq.14)}$$

A admitância vista por TX1/TX2 (após a inserção do circuito de adaptação) vem dada por:

$$Ymax = \frac{R}{R^2+(wL)^2} + \mathrm{j}(\mathrm{wC} - \frac{\mathrm{wL}}{R^2+(wL)^2}) \qquad \textbf{(Eq.15)}$$

Para adaptar o circuito basta fazer Y_{min} igual ao valor da admitância desejada em TX1/TX2. Ou alternativamente utilizam-se as equações 16 e 17 para se obter uma primeira aproximação do filtro.
Prova-se que num circuito de adaptação em malha L idêntico ao utilizado no circuito anterior, com R_t (impedância equivalente) >> R (impedância a adaptar), as seguintes aproximações são válidas [29]:

$$Q = \frac{Wo.L}{R} = \sqrt{\frac{R_t}{R}} \qquad \textbf{(Eq.16)}$$

$$W_0 = \sqrt{\frac{1}{L.C}} \qquad \textbf{(Eq.17)}$$

Os valores dos componentes do circuito podem agora ser calculados:

Da equação 13 vem: $R_{Total} \approx 2.75\ \Omega$, para Q = 25;
Da equação 14 vem: $R_{ext} = 0.65\ \Omega$, sendo $R_{coil} = 2.1\ \Omega$;
Da equação 9 resulta: C1 = 348 pF, com L = 395.5 nH (medido);
Das equações 16 e 17 tiram-se os valores de C0 e L0: L0 = 87 nH e C0 = 1.58 nF, com R_t = 20 Ω;

Optimização recorrendo ao ADS

Com as primeiras aproximações obtidas anteriormente simulou-se o circuito da figura seguinte (metade da antena). A figura Fig. 30 mostra a impedância equivalente e o coeficiente de reflexão da primeira aproximação.

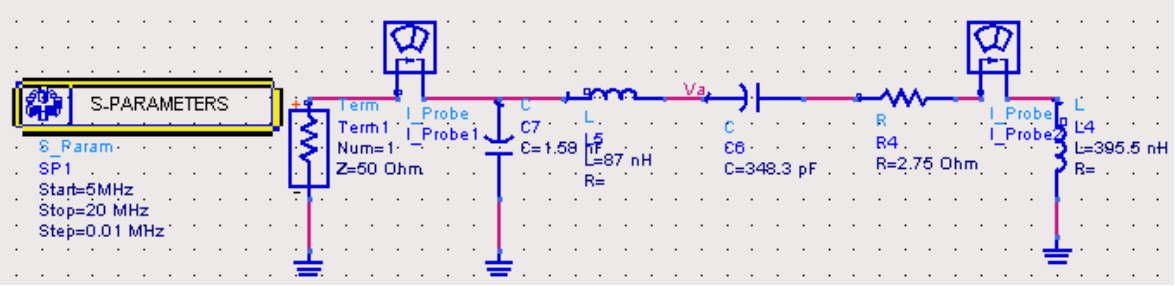


Fig. 29) Metade superior da antena

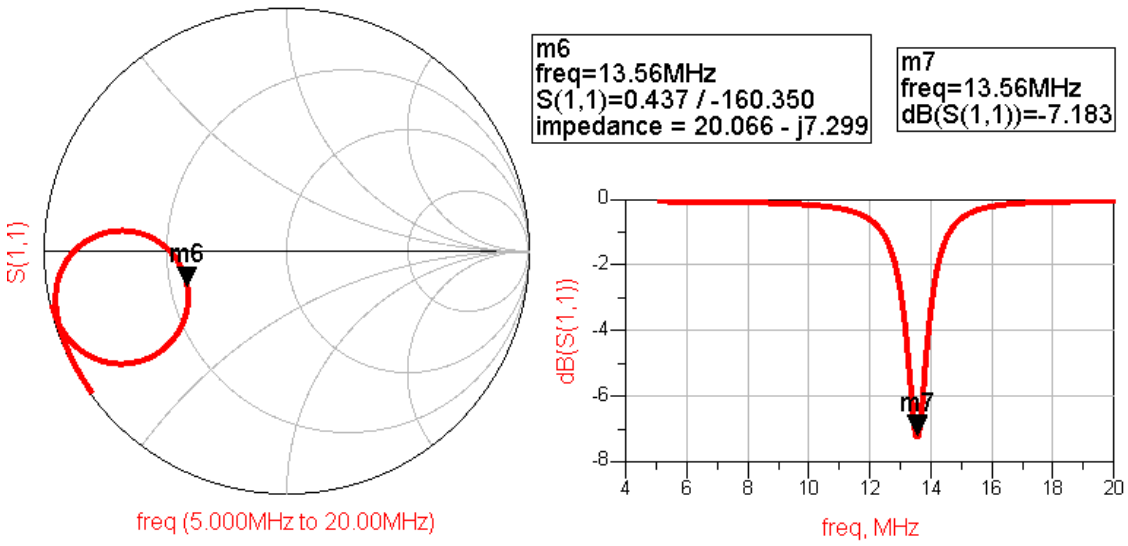


Fig. 30) Impedância equivalente e coeficiente de reflexão da 1ª aproximação

Como se pode ver pela figura anterior o circuito precisa ser optimizado de modo a obter-se o valor desejado para a impedância de entrada da antena. Para isso fez-se variar o valor do condensador C0. Para um novo valor de C0 = 1.372 nF, conseguiu-se uma melhor aproximação de R_t: Z_{min} = 22.689 + j0.882 com S11 = -9.686 dB (Fig. 31).

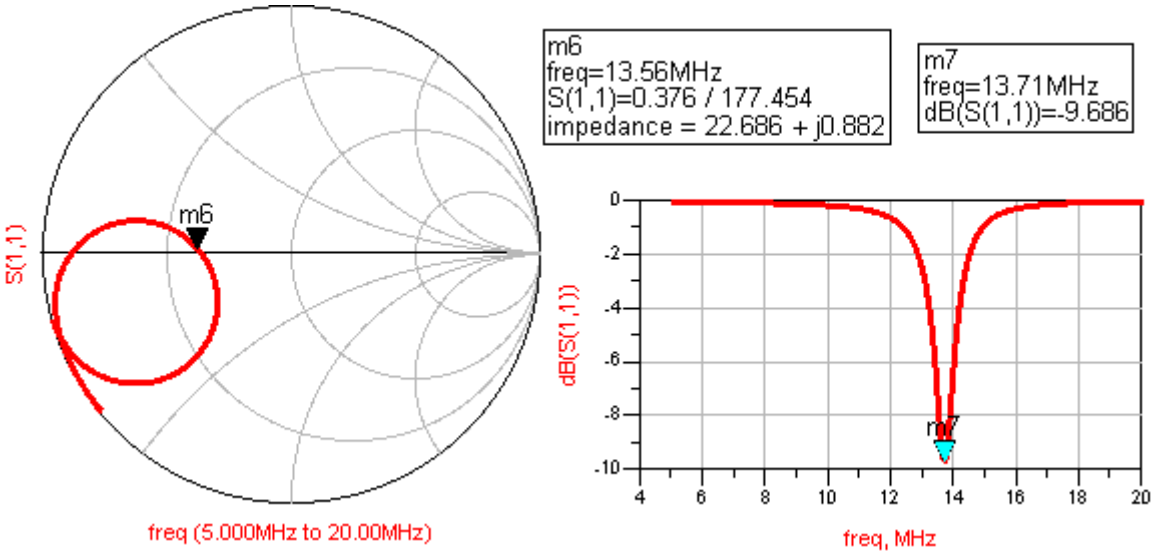


Fig. 31) Impedância equivalente optimizada

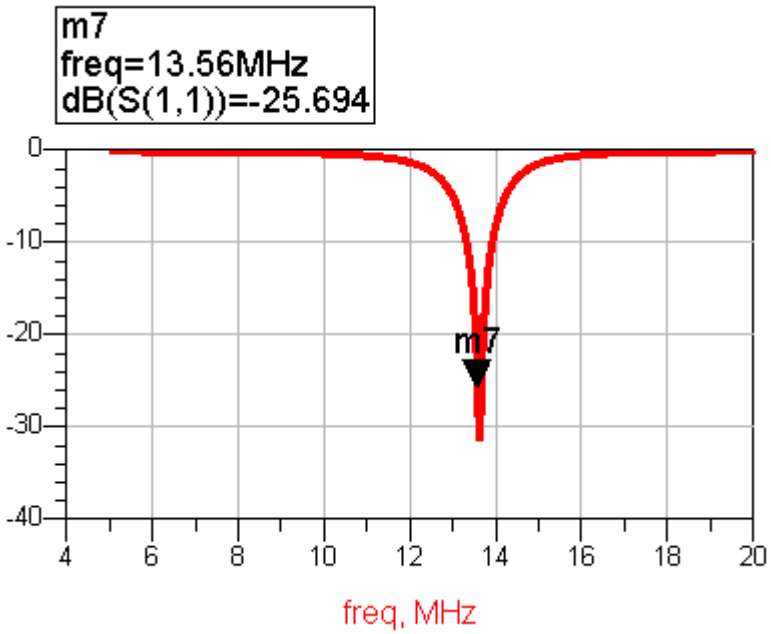


Fig. 32) Coeficiente de reflexão da antena completa (adaptada)

Circuito transmissor completo

A Fig. 33 mostra o circuito completo do transmissor. Este circuito já integra alguma parte da electrónica interna do transceiver (simulado por um gerador binário aleatório a 106Kbps, um oscilador local a 13.56MHz e um misturador). O objectivo é simular o circuito de transmissão e analisar os sinais ao longo da cadeia.

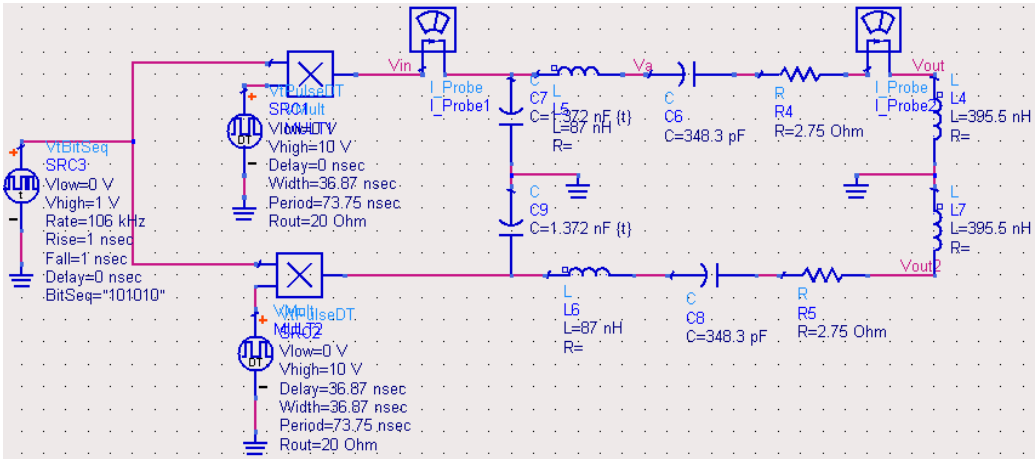


Fig. 33) Circuito transmissor completo

A Fig. 34 mostra à esquerda a tensão e corrente à entrada da antena (pinos TX1 e TX2). A corrente à saída de TX1/TX2 é I = 90.98mA inferior ao valor máximo admitido pelo transceiver (I_{TXmax}=150mA).

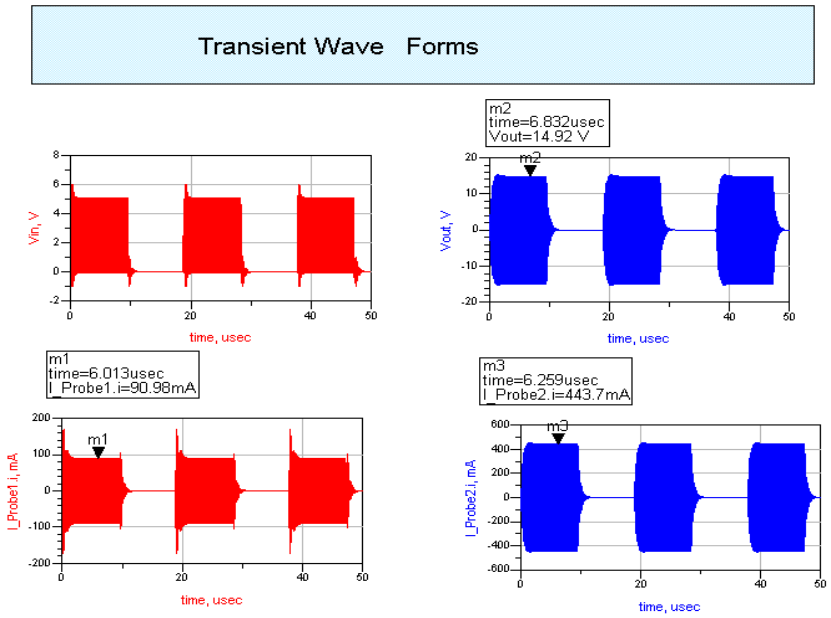


Fig. 34) a) tensão e corrente a entrada da antena; b) Tensão e corrente na bobina da antena

3.5 – 1º Protótipo do leitor

A seguir mostra-se o primeiro protótipo do leitor. Esta versão da placa possui ainda uma resistência e um condensador variáveis cujo objectivo é afinar a adaptação da antena e melhorar o alcance do leitor. Note-se que aqui só se apresenta uma versão já evoluída do protótipo, omitindo as fases de desenvolvimento intermédias. Esta primeira versão utiliza interface RS232 para comunicação com o PC, enquanto a versão final, apresentada na secção seguinte, utiliza interface USB. A implementação do protocolo USB foi feita inteiramente pela Acronym e não faz parte desta dissertação.

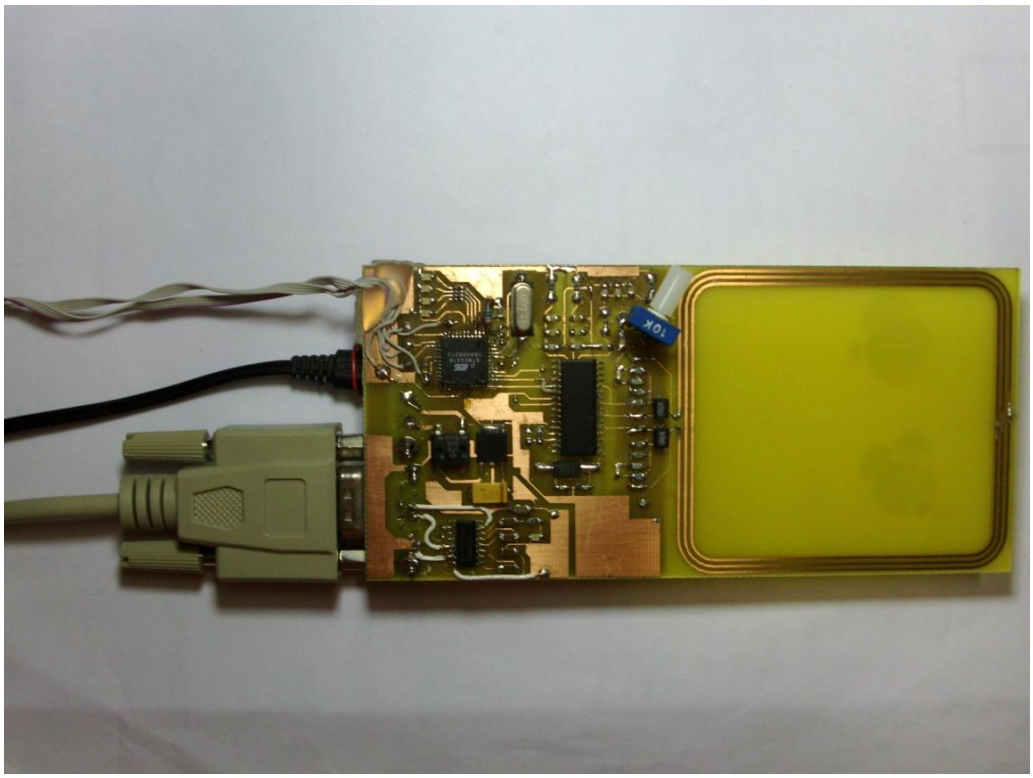


Fig. 35) 1º Protótipo do leitor

3.6 – Versão final

A principal diferença da versão final do leitor em relação ao primeiro protótipo está relacionada com o *firmware*. O *firmware* da versão final do leitor está codificado em Assembly. O código Assembly foi escrito, com a colaboração da Acronym, com base no código em linguagem C anteriormente desenvolvido, no âmbito desta dissertação, para o primeiro protótipo do leitor. Foram feitas algumas optimizações em relação ao código C com vista a facilitar a posterior realização de *multitasking* no uC.

Os *layouts* de ambos os circuitos impressos foram desenhados pela Acronym com base no esquema do circuito eléctrico (em anexo) projectado no âmbito desta dissertação. Procurou-se obter uma versão final da placa de dimensões tão reduzidas quanto possível. Todas as optimizações do *layout* feitas a esse nível foram da responsabilidade da Acronym.

Fig. 36) Versão final do leitor

Capitulo 4 – Desenvolvimento do *Firmware* e da Aplicação

O *firmware* que suporta o protocolo ISO14443-A (Mifare Standard) foi desenvolvido em linguagem C recorrendo ao ambiente de desenvolvimento integrado e compilador AVR Studio da ATMEL. Numa primeira fase foram criadas todas as funções básicas que permitem o acesso ao transceiver, bem como a inicialização, selecção e operações de acesso à memória do transponder. A anti-colisão foi parcialmente implementada. A implementação actual consiste apenas na detecção de colisão e envio de uma mensagem de erro solicitando um único cartão no campo do leitor. Adicionalmente foi criada uma aplicação simples de demonstração correndo no próprio processador *on-board*. Esta aplicação possui interface Hyperterminal/RS232 permitindo ao utilizador, entre outras operações, aceder à memória do transponder para leitura e escrita de blocos.

4.1 – Estrutura do código

A figura seguinte mostra a estrutura do código desenvolvido. O código está seccionado em quatro módulos distintos. O módulo "uart.c" contém as funções responsáveis pela comunicação com o PC via UART. O módulo "spi.c" é responsável pela comunicação MCU-transceiver, permitindo o acesso ao banco de registos do transceiver. Ainda no módulo spi.c, mas num nível superior estão codificadas funções de acesso directo aos registos do transceiver. Estas funções permitem a leitura e escrita transparente de registos do transceiver. Finalmente o módulo "14443protocol.c" implementa o protocolo ISO14443-A, codificando todos os comandos (para o transceiver e para os transponders) necessários para realizar as operações de chamada aos cartões no campo, anti-colisão, selecção de cartão, leitura e escrita de blocos de memória do transponders. O módulo "main.c" contém a interface utilizador que será discutida na secção "Aplicação Demo".

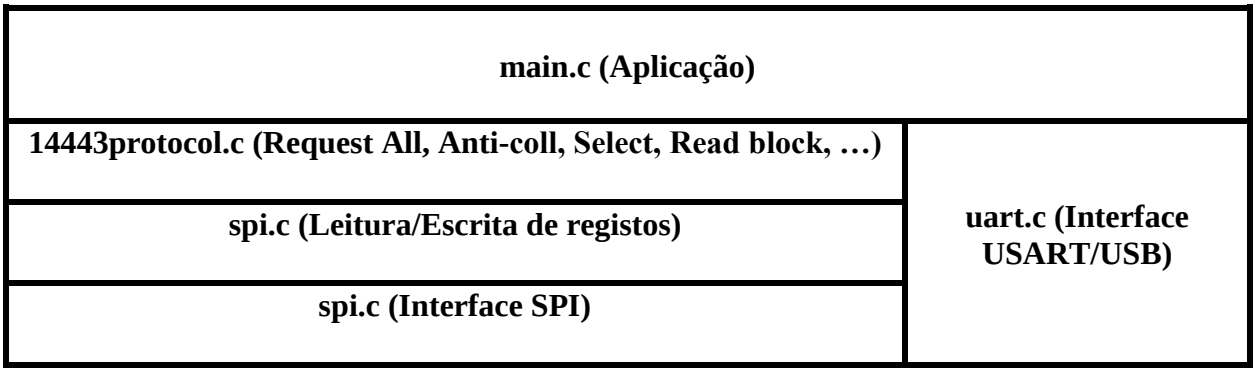


Fig. 37) Estrutura do código

4.2 – Sincronização da comunicação

Do ponto de vista da aplicação, o acesso aos dados guardados no transponder é transparente (Fig. 38). A operação de escrita e leitura de dados do transponder é baseado no princípio de comunicação *master-slave* (Fig. 38). Isto significa que todas as operações realizadas pelo leitor (transceiver) são iniciadas pela aplicação (neste caso pelo MCU *on-board*, uma vez que este aloja a aplicação). A aplicação representa o *master* enquanto o leitor (*slave*) apenas é activado quando recebe um comando da aplicação. Para executar qualquer comando requerido pela aplicação (MCU), o leitor primeiro inicia uma comunicação com o transponder. Nesta segunda etapa, o leitor desempenha o papel de *master* em relação ao transponder, enquanto o transponder opera como *slave* respondendo aos comandos do leitor. Um simples comando da aplicação para o leitor desencadeia um conjunto de comandos do leitor para o transponder (request all, anti-colisão, selecção, leitura/escrita). A figura seguinte mostra o fluxo de dados entre a aplicação (MCU), o leitor (transceiver) e o transponder.

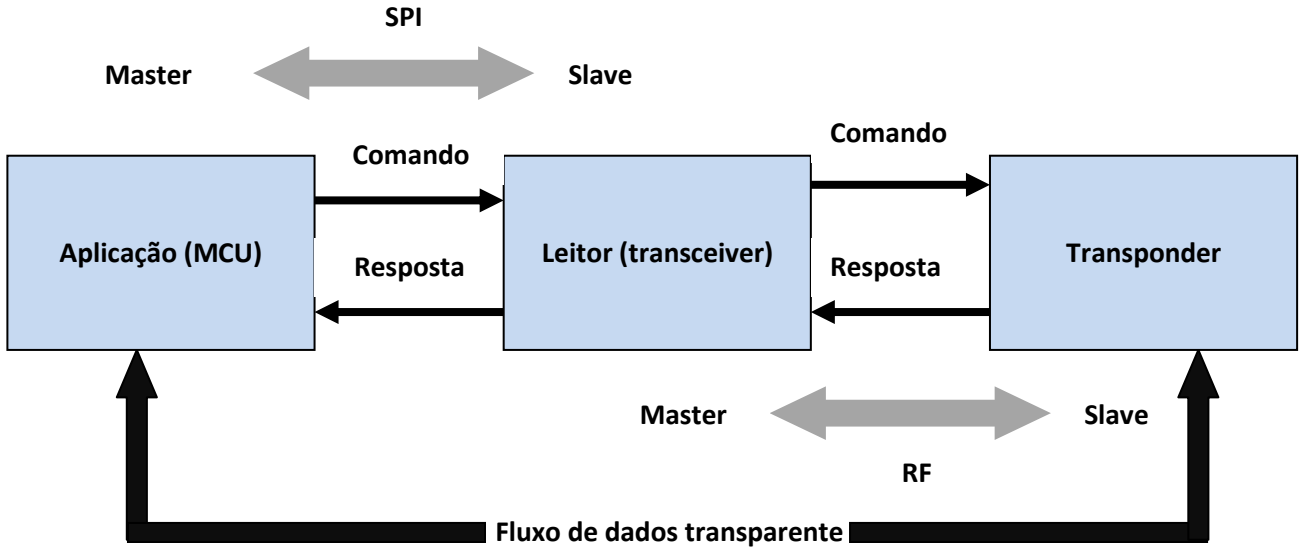


Fig. 38) Fluxo de dados

4.2.1 – Aplicação - leitor

Como já foi referido atrás, a aplicação de demonstração desenvolvida no âmbito desta dissertação corre no próprio MCU do leitor. Porém, na versão final do leitor, a aplicação estará inteiramente alojada no PC. O fluxograma seguinte mostra a interacção entre o *firmware* a correr no leitor e a aplicação a correr no PC. A sequência de operações a realizar é a seguinte:

1- Utilizador inicia a aplicação no PC
2- Inicialização da interface RS232 ou USB
3- A aplicação aguarda até receber uma solicitação do utilizador
4- Uma vez solicitada uma acção, é enviado o respectivo comando ao leitor
   1', 2', 3' e 4' devem ser anteriores a 4.
5- O leitor, que se encontrava à escuta de um comando do PC (5'), já pode prosseguir
6- O leitor executa as operações necessárias para realizar o comando e responde ao PC com dados ou um código de erro, ou com um ACK/NACK

7- A aplicação que aguardava pela resposta do leitor já pode prosseguir
8- A aplicação faz o *display* da resposta recebida do leitor ou usa os dados para processamento

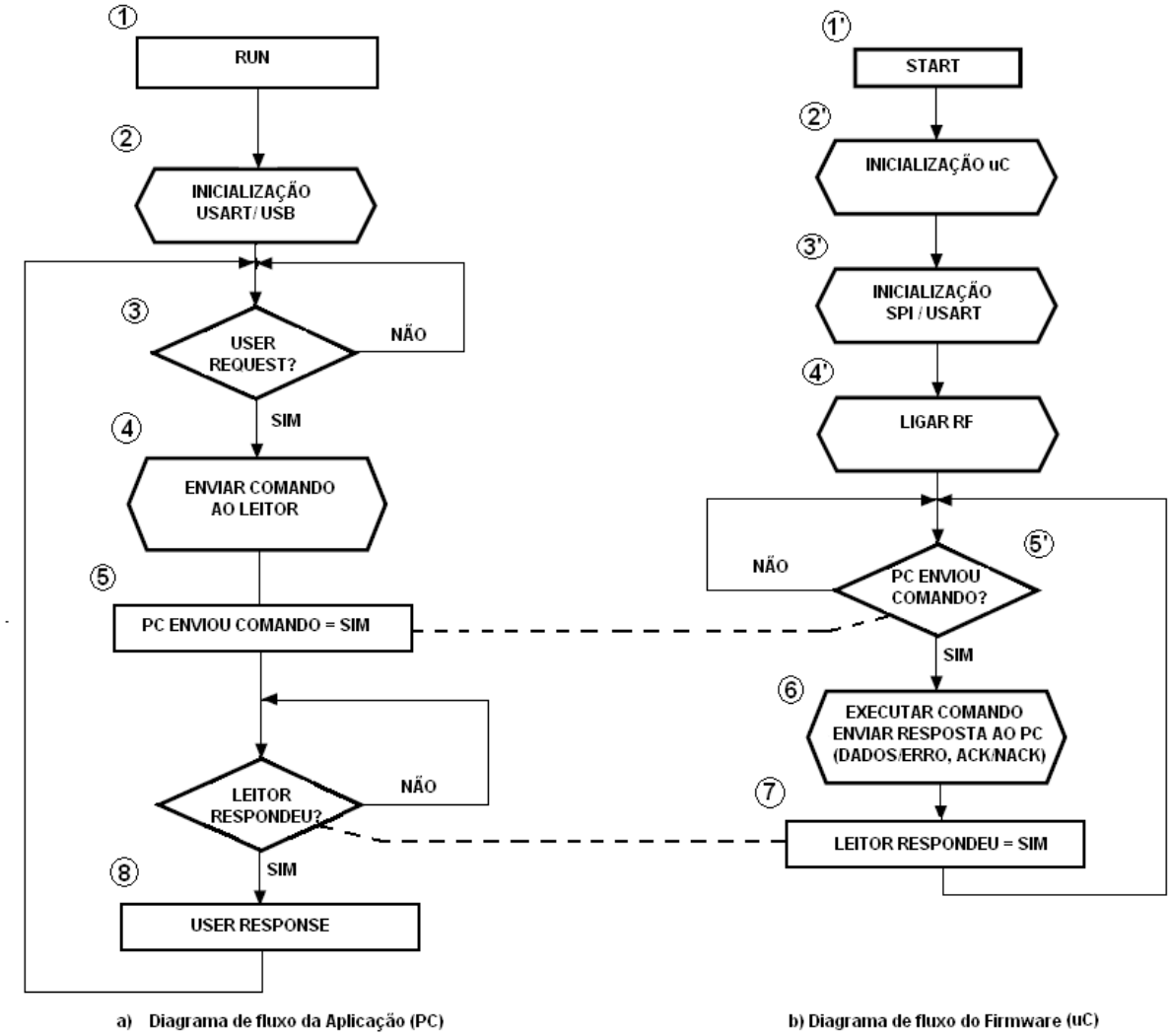


Fig. 39) Fluxograma da aplicação/*firmware*

A etapa 6 corresponde à segunda fase da comunicação. Nesta fase, o leitor passa a desempenhar o papel de *master* enviando comandos ao transponder que opera como *slave* respondendo aos comandos. A descrição desta etapa é feita na secção seguinte.

4.2.2 – Leitor - transponder

Nesta secção pretende-se descrever a implementação da comunicação entre o leitor (MCU + Transceiver) e o transponder. Esta comunicação segue o princípio *master-slave* descrito anteriormente. O leitor envia comandos ao transponder que os interpreta e devolve uma resposta (dados ou erro). Todos os comandos ao cartão implicam comandos ao transceiver. A seguir é listado um conjunto de comandos destinados ao transceiver: IDLE (0x00),

TRANSMIT (0x19), RECEIVE (0x16), TRANSCEIVE (0x1E), AUTHENT1 (0x0C), AUTHENT2 (0x14) e LOAD_KEY (0x19). Alguns exemplos de comandos destinados aos transponders são os seguintes: REQA (0x26), ANTICOLLC1 (0x93), AUTHENT1KA (0x60), READ16 (0x30).

Numa transacção comum, o leitor envia comandos ao transponder e aguarda por uma resposta. Esta resposta poderá ser um NAK (transponder não responde) ou dados armazenados no transponder. O transceiver possui recursos que permitem, por interrupção, detectar algumas ocorrências importantes na interface ar: transmissão concluída (os dados presentes na FIFO foram postos na interface ar), recepção concluída (o cartão respondeu com dados ou com código de erro), ocorrência de *timout* na interface ar (inexistência de cartões no campo ou resposta tardia). Esta última funcionalidade é implementada recorrendo a um *timer* interno do próprio transceiver.

No código desenvolvido, a transacção de dados entre o leitor e o transponder é implementada com base em interrupções sendo assegurada pelas funções PCDCmdRequest (PCD Command Request) e ISR (Interrupt Service Routine) e pelo comando PCD_Transceive (destinado ao transceiver). O comando PCD_Transceive corresponde a uma combinação dos comandos PCD_Transmitt e PCD_Receive. Este comando faz a transmissão dos dados presentes na FIFO do transceiver, aguarda um intervalo de tempo pré-configurado, após o qual inicia a recepção de dados do transponder.

A figura seguinte procura mostrar um possível [4] esquema de comunicação leitor (MCU+transceiver) – transponder.

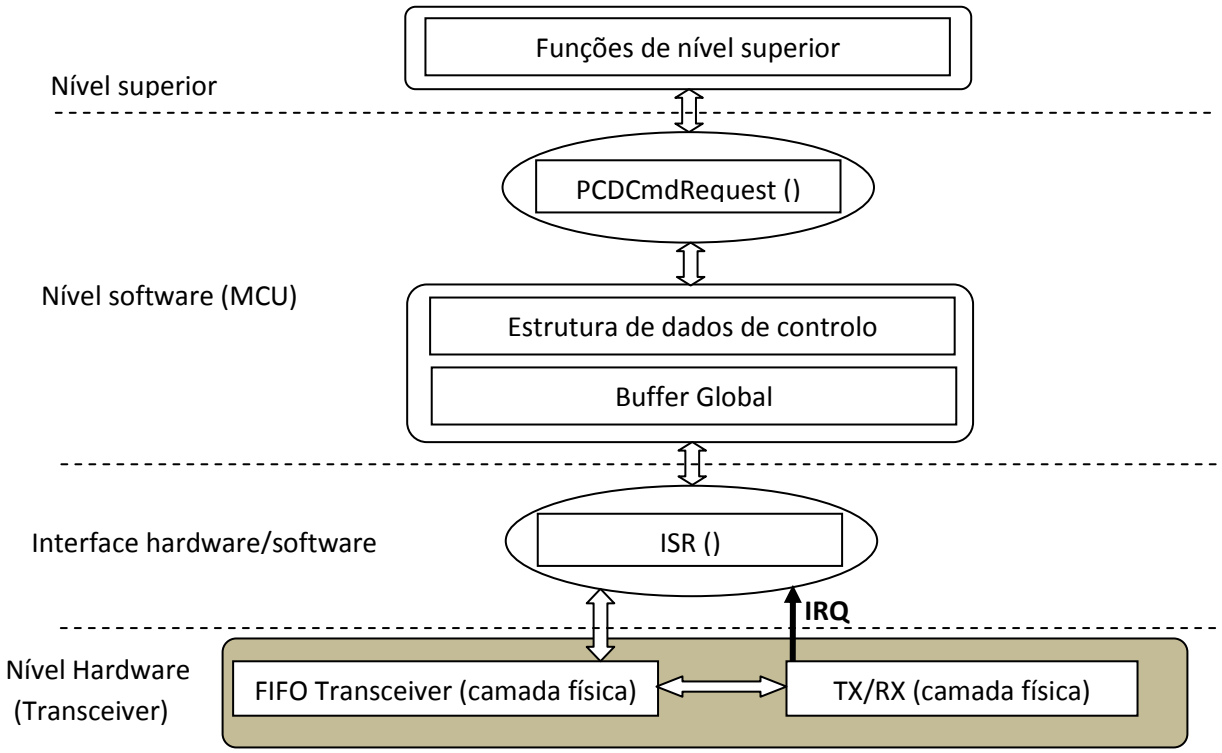


Fig. 40) Comunicação leitor - transponder

[4] Neste projecto, a sincronização da comunicação foi implementada com base em interrupções, uma vez que, o transceiver dispõe de uma linha de interrupção externa. Alternativamente podia-se recorrer ao método de *polling*.

Há uma estrutura de dados global (CMDInfo) contendo informações referentes à própria transacção (comando a executar, status da execução do comando, numero de bytes a enviar/receber do cartão, erros detectados na interface ar, fontes de interrupção, …) e dois buffers globais (SENDERBuffer e RECEIVERBuffer) para troca de dados entre o cartão e o leitor. Estas duas variáveis constituem o canal de comunicação entre a função PCDCmdRequest () e a rotina de serviço a interrupção ISR (). A função PCDCmdRequest (), quando invocada por funções de nível superior, inicia a execução de um comando no transceiver. A PCDCmdRequest () tem a função de carregar os dados do buffer global (previamente disponibilizados pela função invocadora) na FIFO do transceiver, preencher a estrutura de controlo (número de bytes a enviar, comando a executar e status do comando) e iniciar a execução do comando escrevendo o comando TRANSCEIVE no registo COMMAND do transceiver. Após o procedimento anterior, a função PCDCmdRequest (), aguarda pela execução do comando, fazendo *polling* a uma *flag* global. Assim que o comando é executado no nível de hardware (transceiver), é despoletado uma interrupção que é servida pela ISR (). A ISR () tem como função, transpor os dados (recebidos do cartão) do nível físico (FIFO do transceiver) para o nível de software (Buffer global), preencher a estrutura de controlo com informação da transacção (erros, colisão, numero de bytes recebidos, …) e por fim comunicar ao nível de software a execução do comando (através de uma *flag* global).
Uma vez, a função PCDCmdRequest () é informada da execução do comando, esta analisa a estrutura de controlo (erros) e devolve um código de erro a função que a invocou.
Para melhor se compreender a implementação acima descrita, é apresentada no anexo 4 (função Main) uma instanciação do código que visa ler dados do cartão. Pretende-se executar comando READ16 (destinado ao cartão) que lê um bloco de 16 bytes da memória do cartão. Para isso recorre-se a execução, no transceiver, do comando TRANSCEIVE que envia o comando READ16 (código 0x1E) e espera receber 16 bytes de dados do cartão.

4.3 – Implementação do protocolo ISO14443A - Parte3 (Mifare)

Nesta secção vai-se descrever a implementação do protocolo ISO14443A Part3 (Selecção e Anti-colisão) recorrendo a uma sequência de exemplos práticos [17]. Serão mostrados em cada etapa os comandos e dados enviados aos cartões, os dados recebidos e as temporizações necessárias. Será também mostrado o código das principais funções. O exemplo que se apresenta é referente ao cartão Mifare Ultra Light, cuja sequência de comandos pouco difere da dos cartões Mifare 1k e 4k. A principal diferença está no facto deste cartão não requerer autenticação para acesso à memória.

4.3.1 – Inicialização, anti-colisão e selecção do transponder

Qualquer transacção com o cartão é iniciada com o envio do comando REQA (Request All) ou WUPA (Wake Up All). Estes dois comandos têm a idêntica função de acordar todos os cartões no campo de cobertura do leitor. A diferença é que o comando REQA apenas acorda os cartões que entraram pela primeira vez no campo enquanto o WAPA acorda cartões que tenham sido anteriormente adormecidos pelo leitor. O código hexadecimal correspondente ao REQA é 0x26 e o mecanismo de segurança utilizado nesta fase da comunicação é a paridade simples. Os cartões no campo respondem ao REQA com

dois bytes contendo uma codificação própria do fabricante. Trata-se do ATQA (Answer to Request). O cartão Mifare Ultra Light responde com ATQA = 0x44 00, enquanto os cartões Mifare Standard 1k e 4k respondem com ATQA = 0x04 00 e ATQA = 0x02 00 respectivamente. As temporizações necessárias são indicadas na figura seguinte. A inexistência de uma resposta na interface ar, após 260 microsegundos a contar do instante de envio do ATQA deve ser interpretado pelo *firmware* como um *timeout* (inexistência de cartões no campo, ou resposta tardia). A função que implementa o comando REQA é a signed char RequestAll(unsigned char req_code, unsigned char *atq), cujo código é mostrado no anexo 4.

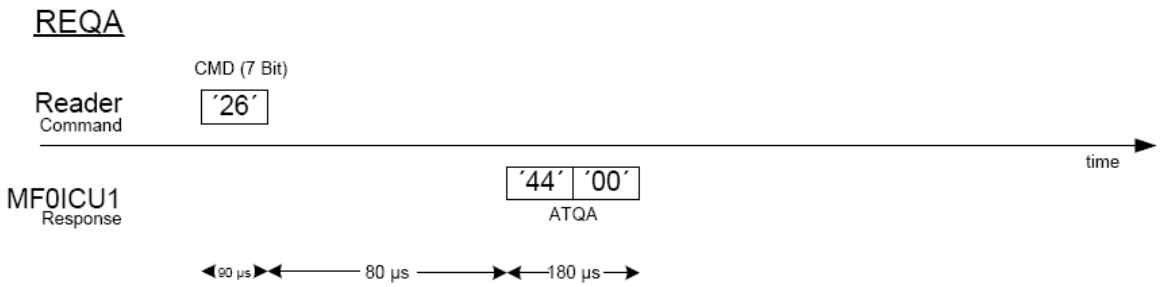


Fig. 41) Protocolo ISO14443A - Comando REQA, retirado de [17]

Pode acontecer que vários transponders estejam no campo do leitor quando este envia o comando REQA. Neste caso todos os transponders no campo respondem à solicitação do leitor, resultando daí uma colisão (Fig. 42).
O transceiver utilizado neste projecto possui recursos de hardware para detectar e resolver colisões, seleccionando um cartão dentre os vários presentes no campo do leitor. No entanto, nesta primeira fase, a anti-colisão não foi implementada. O *firmware* limita-se simplesmente a detectar a ocorrência de colisão (recorrendo a recursos do transceiver) e devolver uma mensagem de erro.

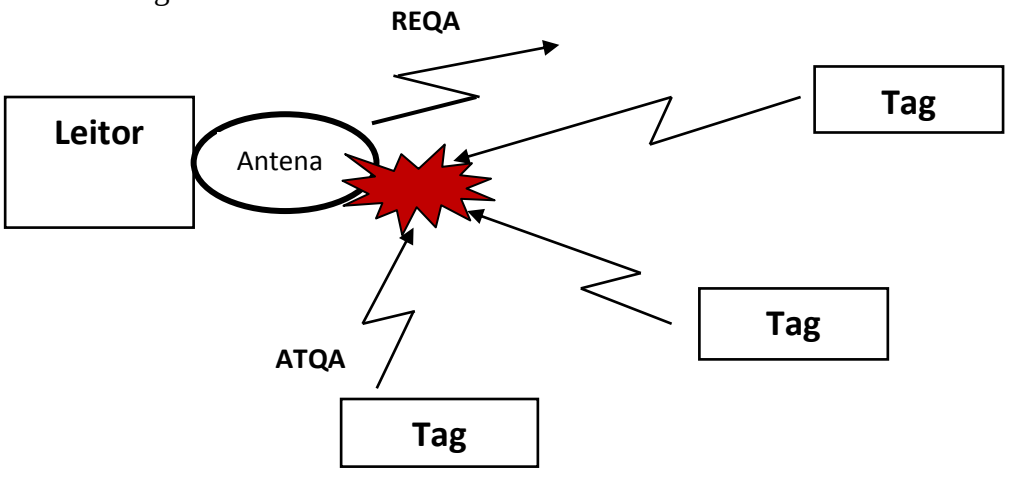


Fig. 42) Colisão na interface ar

A norma ISO14443-A detecta colisões na interface ar de forma extremamente simples. A codificação utilizada em *uplink* (transferência de dados do cartão para o leitor) é a Manchester. Este código permite três sinalizações diferentes: nível lógico "0", nível lógico

"1" e "bit inválido". O nível lógico "0" é representado por uma transição positiva a meio do período de bit enquanto o nível lógico "1" corresponde a uma transição negativa a meio do período de bit. Isto significa que qualquer sinalização válida deve estar durante meio período baixo e durante o meio período seguinte alto ou vice-versa. Qualquer sinal que permaneça todo o período baixo ou alto não constitui uma sinalização válida e é interpretado como "bit inválido". Esta particularidade do código Manchester é utilizada pela norma ISO14443-A para detectar colisões. Se pelo menos dois transponders estiverem no campo aquando da solicitação do leitor, tecnicamente estes irão responder em simultâneo pelo que o sinal RF dos seus identificadores sobrepor-se-á. Uma vez que os transponders possuem identificadores únicos, haverá pelo menos uma posição do sinal sobreposto que violará o código Manchester, sendo esta a posição de colisão. Por outras palavras, havendo pelo menos dois transponders no campo, a sobreposição dos sinais só seria total, não violando assim o código Manchester, se todos os transponders tivessem o mesmo identificador, o que invalida a premissa de unicidade do identificador. A figura seguinte pretende ilustrar a detecção de uma colisão quando dois transponders respondem simultaneamente a solicitação do leitor. Para simplificar, vamos aqui supor que os transponders possuem um identificador de apenas quatro bits. O transponder 1 possui o UID1 = 0b1101 e o transponder 2 o UID2 = 0b1111. O sinal sobreposto que aparece na antena do leitor é igualmente representado, onde se pode verificar uma violação do código Manchester e por isso a ocorrência de uma colisão no segundo bit LSB da sequência sobreposta. No transceiver MFRC531 esta detecção é feita inteiramente por hardware, havendo uma *flag* que sinaliza esta ocorrência.

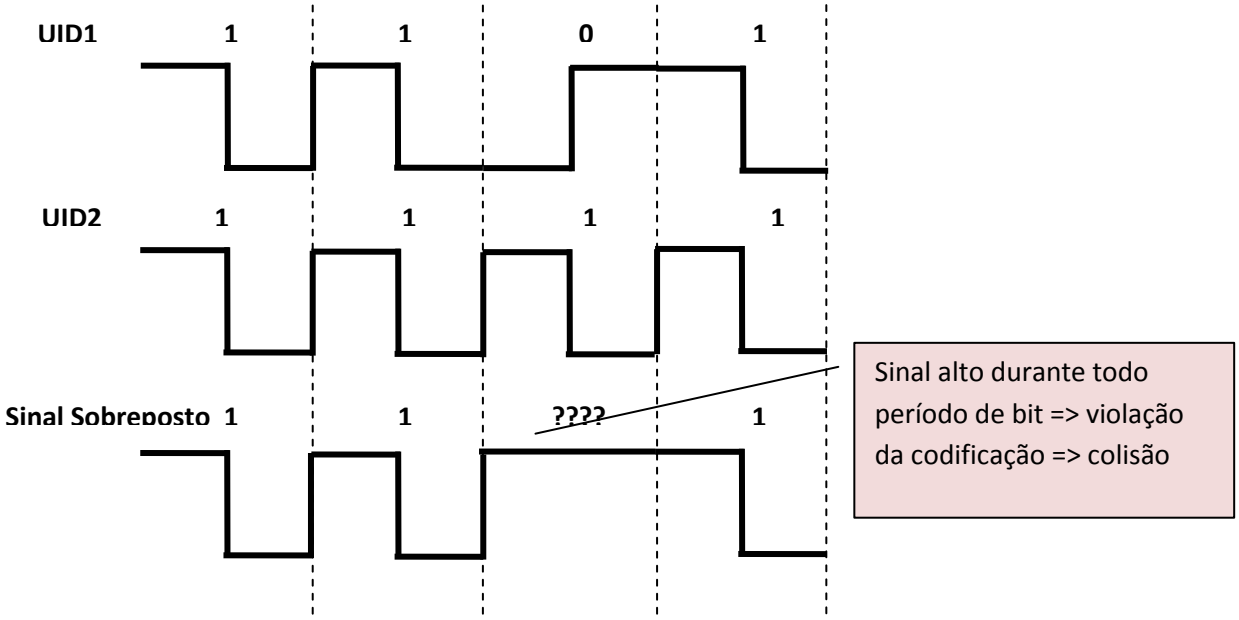


Fig. 43) Detecção de colisão na interface ar (sinais banda-base)

Após a detecção da colisão, deverá ser iniciado o mecanismo anti-colisão de modo a seleccionar-se um único cartão para as operações subsequentes. O mecanismo para resolução de uma colisão encontra-se descrito no anexo 1. Neste projecto, a distância máxima de leitura conseguida foi de cerca de 7-8cm (o transceiver utilizado permite um alcance máximo de 10cm), razão pela qual se desconsiderou a existência simultânea de

vários tags no campo de leitura e não se implementou a anti-colisão. Numa fase posterior, pretende-se projectar um *Front-End* (Amplificador de potência e Amplificador de baixo ruído externos) para melhorar o alcance da antena e nesta altura, o mecanismo anti-colisão já seria justificável.
Quanto ao tamanho do UID, o protocolo ISO14443-A admite três níveis distintos: nível 1 com UID simples (4 bytes), nível 2 com UID duplo (7 bytes) e UID 3com UID triplo (10 bytes). Esta informação está contida no Answer to Request (ATQA). Na arquitectura Mifare, os cartões 1k e 4k possuem UID simples enquanto o Ultra Light possui UID duplo. A anti-colisão e selecção em cada nível é implementado respectivamente com os comandos Anticollision e Select Cascade Level 1, 2 e 3. Neste exemplo, será necessário implementar os níveis 1 e 2 visto estar-se na presença de um UID duplo. No caso dos cartões 1k e 4k bastaria a execução do nível 1. Supondo então a existência de um único transponder no campo de cobertura do leitor, e não havendo portanto a necessidade de resolver colisões, os próximos passes do protocolo consistem em enviar o comando anti-colisão nível 1, código 0x93, argumento 0x20 (Fig. 44), esperar receber os 3 primeiros bytes (SN0, SN1 e SN2) do UID do cartão e validar estes bytes com o comando Select (Fig. 45). Também aqui, o *firmware* deve precaver as situações de *timeout* na interface ar. Os mecanismos de integridade de dados utilizados nesta e nas restantes fases da anti-colisão e selecção são a paridade, o BCC e o CRC na operação de selecção. O BCC consiste em um byte que resulta do *exclusive-or* de todos os bytes a enviar.

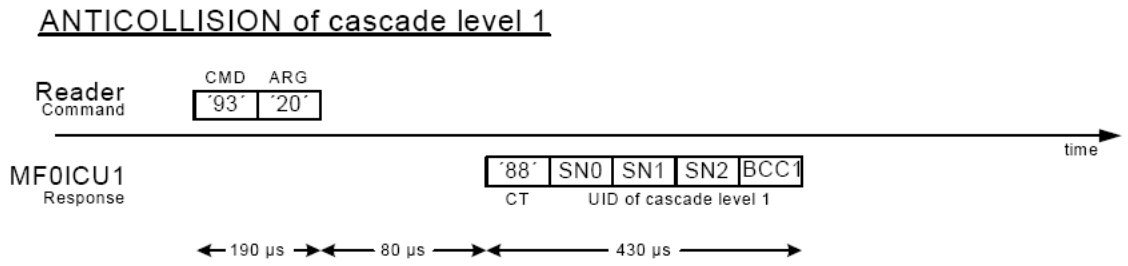


Fig. 44) Protocolo ISO14443A - Comando ANTICOLLC1 nível 1

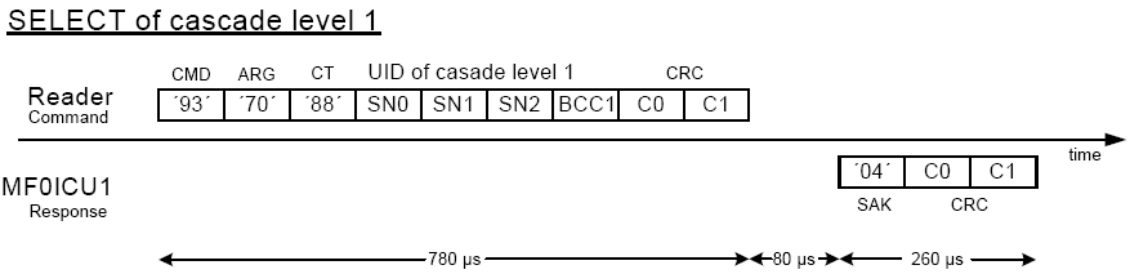


Fig. 45) Protocolo ISO14443A - Comando SELECTC1 nível 1

Se estivéssemos na presença de um cartão com UID simples, os 4 primeiros bytes da resposta ao comando Anticollc1 (Fig. 44) representavam o UID completo do cartão. Estando na presença de um UID duplo o procedimento anterior deve ser repetido, agora

com os comandos Anticollc2 (código 0x95 e argumento 0x20) e Selectc2 (código 0x95 e argumento 0x70) para se poder validar os restantes 4 bytes do UID (Fig. 46).

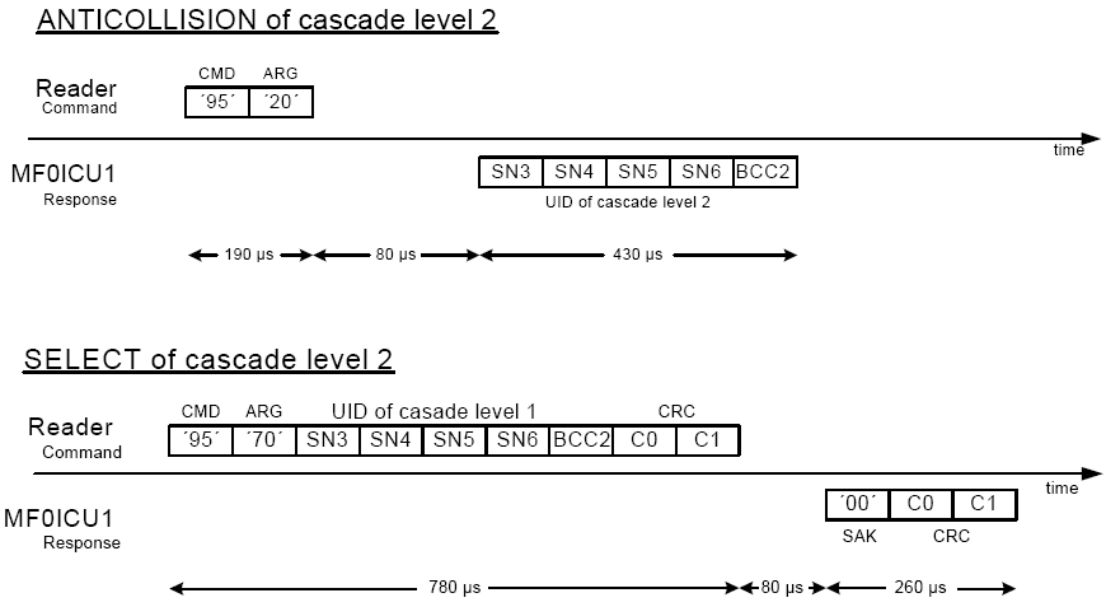


Fig. 46) Protocolo ISO14443A - Comandos ANTICOLLC2 e SELECTC2 nível 2

A função que realiza a anti-colisão multi-nível é a signed char MultiLevelAnticoll(unsigned char cascad_anticol, unsigned char *snr) e o seu código é mostrado no anexo 4. Dependendo do primeiro parâmetro de entrada (cascad_anticol), esta função executa um dos três níveis anti-colisão e devolve em snr o ponteiro para o UID do cartão.
Já a selecção dos transponders é realizada pela função signed char MultiLevelSelect (unsigned char select_code, unsigned char *snr, unsigned char *ats), cujo código se encontra no anexo 4. Esta função recebe o UID e o nível a validar (select_code) e faz a selecção do respectivo nível.

4.3.2 – Operações de leitura e escrita na memória

Uma vez enviado o comando select de nível mais elevado, o cartão terá já devolvido o seu UID completo. No caso do Ultra Light, após dois níveis de Anti-colisão e Selecção, o firmware dispõe do UID = SN6 SN5 SN4 SN3 SN2 SN1 SN0. Na posse do UID, o firmware pode realizar operações de acesso à memória. Nos cartões 1K e 4K, é necessária uma etapa adicional de autenticação do leitor através dos comandos AUTHENTKA ou AUTHENTKB. Para isso o firmware deverá possuir a *password* do sector de memória a que se pretende aceder.
Os cartões Ultra Light não exigem autenticação para acesso à memória, pelo que nesta fase o leitor está em condições de aceder directamente à memória do cartão. São permitidas operações de leitura e escrita de blocos de dados da memória. Neste exemplo, efectuar-se-á apenas a leitura de um bloco de memória do cartão (Fig. 47).

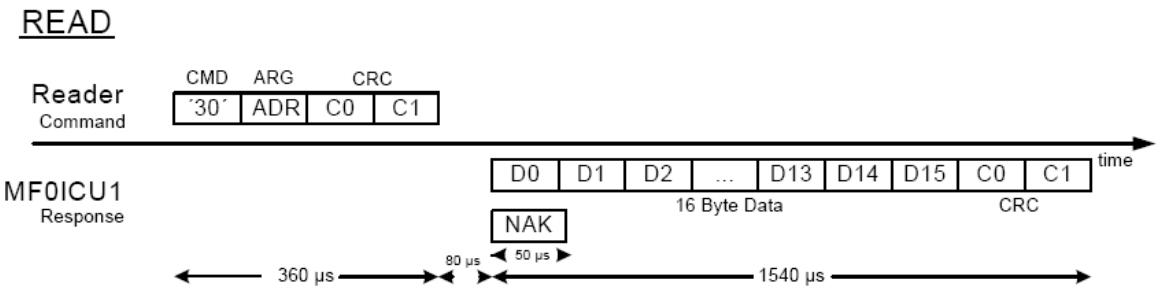


Fig. 47) Protocolo ISO14443A - Comando Read, leitura da memória

Para leitura de dados da memória do cartão, o leitor deverá enviar quatro bytes: o código do comando READ (0x30), o endereço do bloco a ler e dois bytes de CRC que são computados em hardware. Após 80 microsegundos o cartão deverá responder com os 16bytes guardados no endereço solicitado ou com um *Not Acknowledgement* (NAK). O NAK é interpretado como a não recepção de 16 bytes de dados e acontece numa das seguintes situações: operação não permitida, comando ou endereço inválido ou erro na interface ar. Numa operação de leitura bem sucedida, o cartão devolve os 16 bytes de dados seguidos de dois bytes de *cheksum* (C0 e C1). A função signed char ReadPICCDataBlock(unsigned char addr, unsigned char *data) é apresentada no anexo 4. Esta função recebe o endereço do bloco a ler e devolve em data o ponteiro para os 16 bytes recebidos.

A tabela seguinte resume a sequência de comandos necessária para efectuar uma escrita seguida de uma leitura na memória de um cartão Mifare standard 1k. A principal diferença em relação ao exemplo anterior (cartão Ultra Light) é a necessidade de autenticação para acesso à memória do cartão. Após uma autenticação bem sucedida, todas as transacções leitor-cartão são encriptadas. Outra diferença é o UID que nos cartões Mifare Standard é simples (4bytes). Na tabela omitem-se os bytes redundantes de paridade. O UID utilizado neste exemplo é meramente ilustrativo.

Downlink			**Uplink**
Comando	**Código Hexadecimal**	**Argumentos/Dados a enviar**	**Dados recebidos do cartão**
REQA	0x26	----------	0x 04 00 (ATQA)
ANTICOLLC1	0x93	0x20	0x 2A 69 8D 43 (UID do cartão)
SELECTC1	0x93	0x70 0x 2A 69 8D 43 8D	0x08 (ATS)
AUTHENTKA	0x60	0x04 (endereço memória)	----------
WRITE16 (PART1)	0xA0	0x04 (endereço memória)	---------- (cartão não deve responder)
WRITE16 (PART2)	----------	D0 D1……D15 (dados a escrever na memória)	AK
READ16	0x30	0x04 (endereço memória)	D0 D1……D15 (dados)

Tabela 5) Exemplo de escrita seguida de leitura num cartão Mifare Standard

4.4 – Descrição sucinta das funções desenvolvidas

A tabela seguinte mostra as funções desenvolvidas neste projecto. A maioria das funções devolve um código de erro (valor negativo) indicando o tipo de erro que ocorreu durante a sua execução. A avaliação do erro deve ser feita pela função invocadora.

Função	Descrição
MÓDULO UART.C	
void ***uart_config****(void)*	*Configura a usart para modo assíncrono, baude rate de 57600 bps, 8 bits/frame e 1 stop bit*
void ***send_char****(unsigned char data)*	*Envia o carácter (8 bits) data via uart*
unsigned char receive_char(void)	*Recebe um carácter via uart*
void ***print_string****(unsigned char *str)*	*Imprime em Hyperterminal uma string cujo ponteiro é passado como parâmetro em str*
void ***print_number****(unsigned char base, unsigned int val)*	*Imprime em Hyperterminal o valor val na base base. É útil para o display de valores hexadecimais*
void ***read_ascii_string****(unsigned char * str)*	*Input de strings em formato ASCII do teclado (via uart)*
void ***read_hex_string****(unsigned char *str, unsigned char length)*	*Input de strings em formato hexadecimal, cujo comprimento length é conhecido.*
void ***read_password****(unsigned char *key)*	*Input transparente de passwords para acesso a memória dos transponders.*
void ***read_data****(unsigned char *data)*	*Input de dados a serem gravados no transponder*
MÓDULO SPI.C	
void ***spi_master_config****(void)*	*Configura e inicializa o módulo SPI do microcontrolador como master*
unsigned char ***spi_transceive_byte_r****(unsigned char byte)*	*Faz o transceive de um byte via SPI. Destina-se a operação de leitura de registos do slave (transceiver)*
void ***spi_transceive_byte_w****(unsigned char byte)*	*Faz o transceive de um byte via SPI. Destina-se a operação de escrita de registos no slave*
unsigned char ***ReadReg****(unsigned char address)*	*Lê o registo address do transceiver e devolve o seu valor*
void ***WriteReg****(unsigned char address,unsigned char value)*	*Escreve o valor value no registo address do transceiver*
MÓDULO 14443PROTOCOL.C	
void ***pcd_start_Up****(void)*	*Executa a fase de inicialização do transceiver*
void ***SetBitMask****(unsigned char reg,unsigned char mask)*	*Coloca a 1 todos os bits do registo reg indicados na mascara mask.*
void ***ClearBitMask****(unsigned char*	*Coloca a 0 todos os bits do registo reg*

reg,unsigned char mask)	indicados na mascara mask. Útil para operações nos registos do transceiver
unsigned char **IsBitSet**(unsigned char val,unsigned char pos)	Devolve verdadeiro se o bit da posição pos do byte val for 1
void **wait_100Us**(unsigned long n_microsec)	Delay de aproximadamente n_microsec*100 us. Útil para gerir as temporizações do protocolo
void **SetIso14443A**(void)	Configura o transceiver para operar de acordo com a norma ISO14443 Tipo A, ajustando o codificador, descodificador, receptor, transmissor, modulador e desmodulador.
void **turnON_RF**(void)	Liga o campo RF
void **turnOFF_RF**(void)	Desliga o campo RF
void **FlushFIFO**(void)	Limpa a FIFO do transceiver
void **StartTimerNow**(void)	Configura e arranca imediatamente o Timer interno do transceiver
void **StopTimerNow**(void)	Para imediatamente o Timer interno do transceiver
void **Set_Timer**(unsigned long numberOfEtus)	Configura o timer do transceiver para arrancar no inicio de uma transmissão na interface RF, parar no final da recepção ou gerar uma interrupção após numberOfEtus ETUs. 1ETU=74ns. Útil para implementar as temporizações do protocolo e detectar timeout na interface RF
void **ISR_conf**(void)	Configura simultaneamente a Interrupção do microcontrolador e do transceiver
signed char **PCDCmdRequest**(unsigned char cmd)	Esta função solícita a execução de comandos ao transceiver, aguarda pela sua execução e avalia e devolve erros a função que a invocou. Esta função juntamente com a ISR implementam a interface transceiver/transponder - microcontrolador
ISR(INT0_vect)	Rotina de serviço a interrupção. Serve todas as interrupções despoletadas pelo transceiver
signed char **RequestAll**(unsigned char req_code, unsigned char *atq)	De acordo com o valor de req_code, envia para o ar os comandos REQA ou WAPA destinados ao transponder. Devolve em atq o ATQA do transponder
signed char **MultiLevelAnticoll**(unsigned char cascad_anticol,unsigned char *snr)	De acordo com o valor de cascade_anticol, executa um dos três níveis anti-colisão. Devolve em snr o UID do respectivo nível
signed char **MultiLevelSelect**(unsigned char	De acordo com o valor de select_code,

select_code,unsigned char *snr,unsigned char *ats)	executa um dos três níveis de selecção. Devolve em snr o UID do respectivo nível
unsigned char **UIDSize**(unsigned char * atq)	Identifica o tipo de UID (simples, duplo ou triplo) através do ATQA recebido do cartão. Esta informação é útil no mecanismo de anti-colisão
unsigned char **CardType**(unsigned char * atq)	Identifica o tipo de cartão (Mifare 1k, Mifare 4k ou Mifare Ultra Light)
signed char **ActivateCard**(unsigned char * uid,unsigned char * uid_length,unsigned char * cardType, unsigned char card_request_code)	Esta função combina as funções MultiLevelAnticoll e MultiLevelSelect para activar um cartão. Precisa de informações relativas ao tipo de UID e de cartão.
void **CodeKey**(unsigned char *key,unsigned char *coded_key)	Faz a codificação das passwords de acordo com o formato requerido pelo transceiver. Recebe a password de 6 bytes em key e devolve-a codificada em 12 bytes em coded_key
signed char **Authenticate**(unsigned char mode,unsigned char *uid,unsigned char *key,unsigned char block_number)	Executa a autenticação do leitor com o cartão em modo A ou B consoante o valor de mode. Esta função recebe o UID do cartão, o endereço (numero) do bloco e a password
signed char **ReadPICCDataBlock**(unsigned char addr,unsigned char *data)	Lê 16 bytes de dados do cartão. Recebe o endereço a ler e devolve em data o ponteiro para os 16 bytes de dados.
signed char **WritePICCDataBlock**(unsigned char addr,unsigned char *data)	Escreve 16 bytes de dados no bloco addr do cartão
signed char **ChangeSectorPassword**(unsigned char *selected_uid, unsigned char sector_number, unsigned char *old_pass,unsigned char *new_pass)	Modifica a password de um determinado sector de memória do cartão. Requer a password actual do sector
signed char **GetBlockAccess**(unsigned char *selected_uid,unsigned char block_add, unsigned char *key,unsigned char * access)	Lê as condições de acesso de um dado bloco de memória. As condições de acesso determinam as permissões de leitura e escrita do bloco e o modo de autenticação (A ou B) exigido
signed char **WriteBlockAccess**(unsigned char *selected_uid, unsigned char block_add, unsigned char *key, unsigned char access)	Escreve as condições de acesso de um dado bloco de memória. Nem todas as condições são possíveis (Ex: tornar legível a chave A).

Tabela 6) Descrição das funções desenvolvidas

4.5 – Aplicação Demo

A aplicação de demonstração funciona por defeito em modo de captura permanente. Isto significa que, periodicamente, o leitor envia comandos para a interface ar solicitando os cartões no campo. Assim que é detectado um cartão no campo, o seu UID é mostrado no ecrã. O utilizador poderá optar por continuar neste modo ou entrar em modo MENU clicando em qualquer tecla. O modo de MENU permite operações de leitura e escrita na memória do cartão, modificação de *password* e escrita de condições de acesso. Há também a possibilidade de escrita e leitura da memória dos cartões em formato ASCII. No modo MENU, uma vez que se efectuam operações na memória do cartão, é necessário manter o cartão no campo de cobertura do leitor. A Fig. 48 mostra o modo de captura.

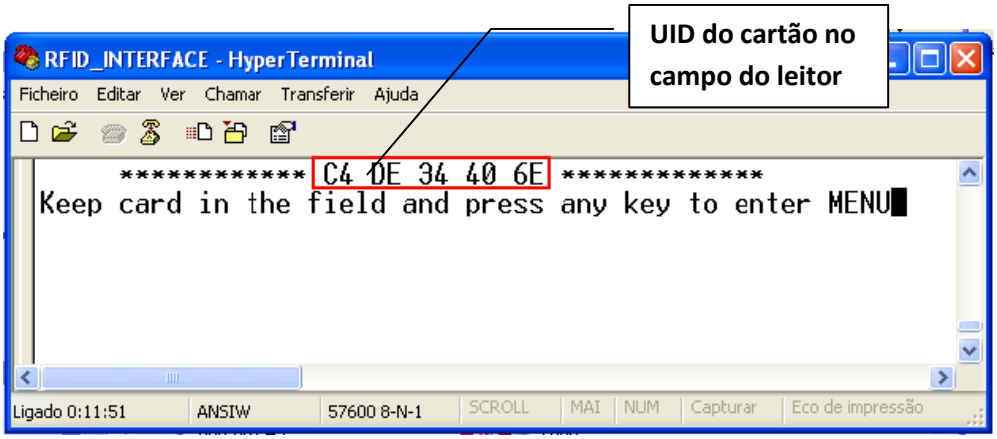


Fig. 48) Aplicação Demo - Modo de captura

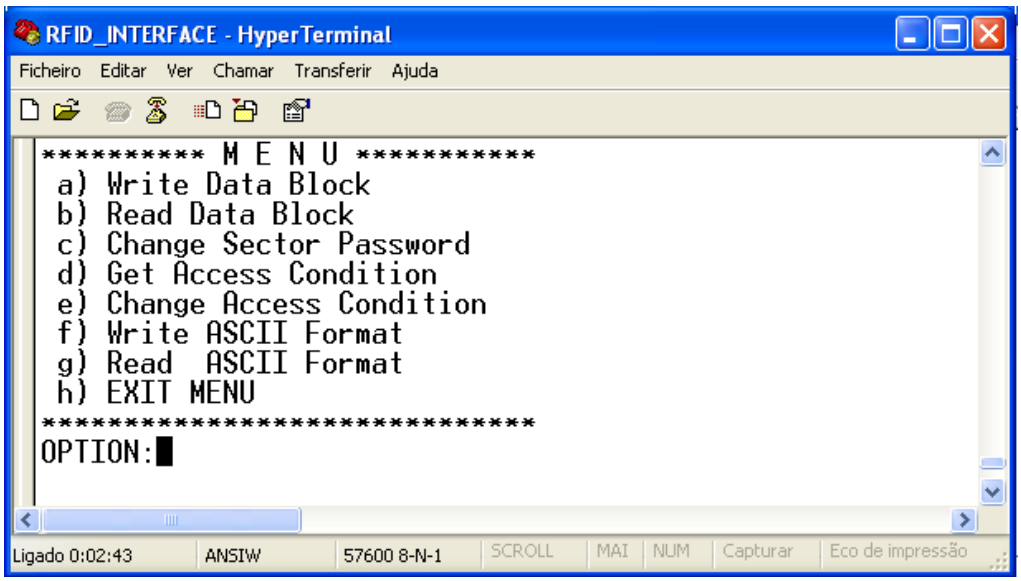


Fig. 49) Aplicação Demo - Modo Menu

Mantendo o cartão no campo do leitor e pressionando qualquer tecla, a aplicação entra em modo MENU (Fig. 49). Trata-se de uma interface de comandos que permite efectuar as operações listadas na figura seguinte. Cada um dos comandos corresponde à invocação da função com o mesmo nome descrita na tabela 6. Todos os argumentos necessários à invocação das respectivas funções, incluindo as *passwords* de acesso, são passados na linha de comandos.

Capítulo 5 – Medidas e testes

5.1 – Estudo e caracterização da bobina da antena

A adaptação da antena, proposta neste projecto, é baseada numa análise isolada da antena do leitor, isto é, não se considera o efeito de carga do transponder na antena do leitor. Este efeito podia perfeitamente ser previsto teoricamente se se conhecesse em pormenor a constituição do transponder, nomeadamente a sua impedância equivalente. Não a conhecendo, há que prever minimamente, medir e tentar minimizar este efeito, sob pena de que a entrada do transponder no campo da antena provoque a dessintonia/desadaptação da antena do leitor.
Nesta secção é analisado, experimentalmente, o comportamento de diversas bobinas: em PCB e em fio, com diversos formatos e dimensões. É feita ainda uma análise do efeito da carga do transponder com o objectivo de se escolher a antena mais adequada.
A metodologia utilizada consiste na utilização de um analisador de redes de quadripólos para medir a impedância e coeficiente de reflexão das diversas bobines (com e sem efeito de carga do transponder) e posterior analise dos resultados no ADS (Advanced Design System). Para isso as medidas retiradas do medidor foram importados para o ADS onde foi feita uma análise de parâmetros S.
À partida sabe-se que quanto maior for o número de espiras, maior será a indutância da bobina. A ideia aqui é estudar qual o impacto real que o cartão (transponder), no campo, tem na impedância e consequentemente no factor de qualidade das diversas bobinas em estudo. Escolher-se-á a bobina (formato, material e numero de espiras) que se mostrar mais "constante" à presença do transponder. A seguir apresentam-se os gráficos dos coeficientes de reflexão (impedâncias) medidos para as diversas condições.
Os três primeiros gráficos mostram os coeficientes de reflexão de bobinas de fio com 2, 3 e 4 espiras respectivamente. Trata-se de bobinas com formato circular de 8 cm de diâmetro. O gráfico da esquerda corresponde à ausência de carga, isto é, não há transponder no campo da bobina. À direita pode-se ver o efeito de carga do transponder na bobina em análise. O mínimo verificado no gráfico da direita corresponde à ressonância do transponder. Como se pode ver, esta ressonância acontece a 16.4MHz, 2.85MHz acima da frequência de operação do sistema. Realmente os transponders estão sintonizados a uma frequência mais elevada (15 - 18MHz) do que a frequência de operação do sistema [5]. Esta opção é seguida nos sistemas que suportam anti-colisão (possibilidade de vários transponders no campo simultaneamente) para minimizar e compensar a influência mútua entre os transponders. Na prática constatou-se que, com dois transponders no campo, a

frequência a que se dá o mínimo de ressonância diminuía e que se aproximava da frequência de operação do sistema (13.56MHz) à medida que se aumentava o número de transponders no campo.
As bobinas de fio aqui analisadas, quando comparadas com as de PCB, apresentam uma grande sensibilidade à presença dos transponders como se pode ver pelos gráficos. Constata-se que, apesar das bobinas de fio apresentarem factores de qualidade mais elevados na ausência do transponder, este degrada-se rapidamente com a entrada do transponder no campo passando a valores muito baixos. Uma vez que a parte reactiva da impedância equivalente (e consequentemente a indutância) da bobina mantém-se praticamente constante (a 13.56MHz) e a parte resistiva altera-se significativamente com a presença do transponder (variações de até 80Ω), há uma grande variação no factor de qualidade da bobina o que não é positivo.

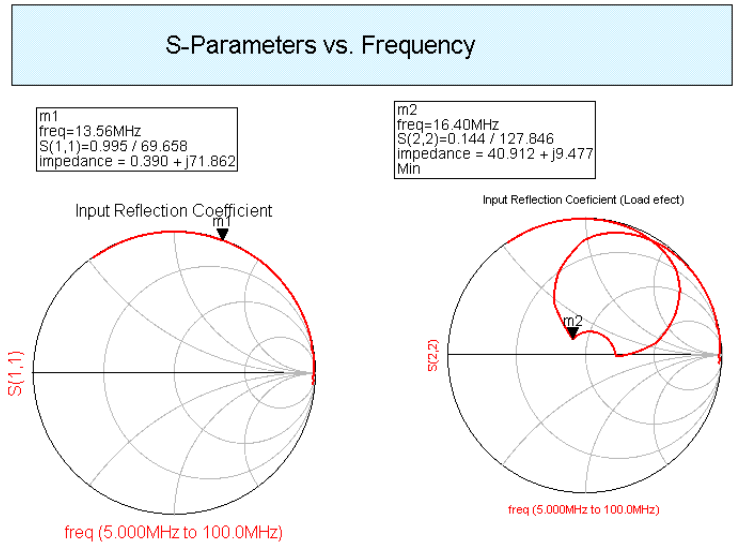


Fig. 50) Bobina 2 espiras de fio. a) sem efeito carga; b) com efeito carga

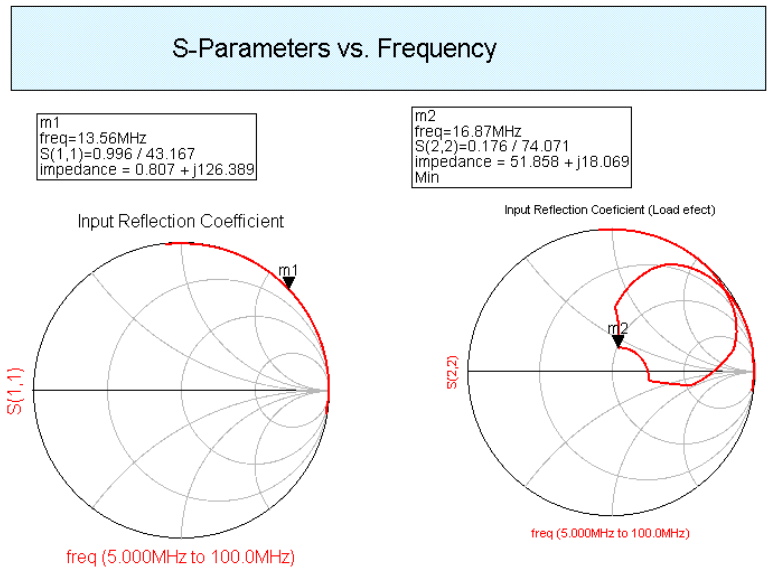


Fig. 51) Bobina 3 espiras de fio. a) sem o efeito carga; b) com efeito carga

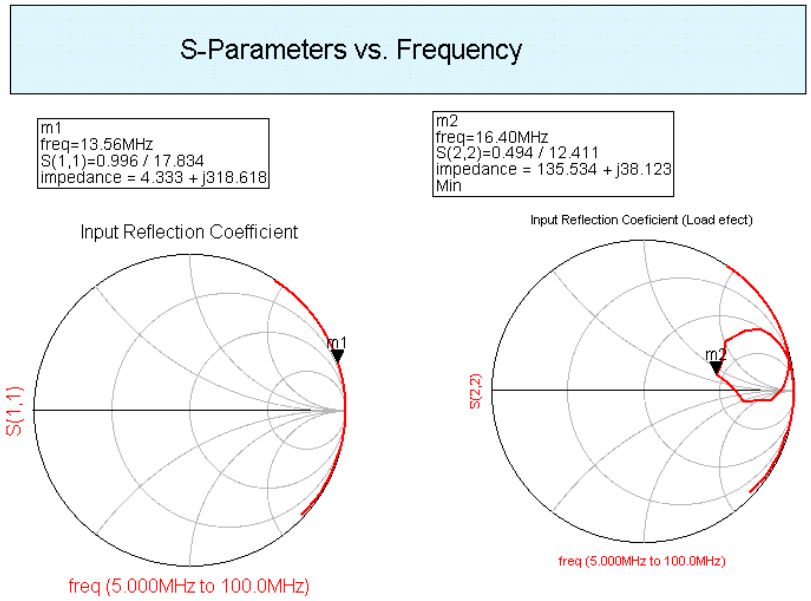


Fig. 52) Bobina 4 espiras de fio. a) sem efeito carga; b) com efeito carga

As figuras seguintes mostram os coeficientes de reflexão (e impedância) de bobinas em PCB (formato rectangular) com 2 e 3 espiras respectivamente. Verifica-se também aqui, o efeito de carga do transponder no gráfico da direita, no entanto, a variação da impedância (devido à presença do transponder) é muito menor que nas bobinas de fio. Apesar das bobinas em PCB apresentarem factores de qualidade inferiores aos das bobinas de fio, as primeiras são mais "imperturbáveis" à presença do transponder. Como já seria de esperar, quanto maior é o numero de espiras, maior é a indutância da bobina (L é proporcional a N – número de espiras). Em contrapartida quanto maior é o número de espiras, maior é o efeito de carga do transponder, degradando o factor de qualidade da bobina do leitor. Isto porque, devido ao efeito transformador a impedância (considerada puramente real) do transponder reflectida no primário (bobina do leitor) vem agravada de um factor de N^2, sendo N a relação de transformação.

Assim sendo, é preciso achar um compromisso entre o número de espiras (efeito de carga do transponder/degradação do factor de qualidade) e a indutância recomendada para a bobina. Optou-se pela bobina em PCB de 3 espiras (Fig. 54). Esta apresenta uma indutância, sem carga, L = 781nH, e com carga L = 833.5nH. Estes valores estão dentro da gama recomendada pelo fabricante do transceiver (0.5 – 3uH) e não apresentam grande variação (com a presença do transponder). O factor de qualidade sem o efeito do transponder vem dado por Q = 32.79 e com o efeito de carga vem Q = 27.78, não havendo degradação significativa de Q. Isto pode ser constatado observando-se as figuras 31 e 32. Aparte a ressonância provocada pela presença do transponder, a curva do coeficiente de reflexão mantêm-se imperturbável. Para além das vantagens apresentadas anteriormente a solução em PCB permite construir uma bobina mais compacta e robusta, para além de reduzir o custo de produção do leitor.

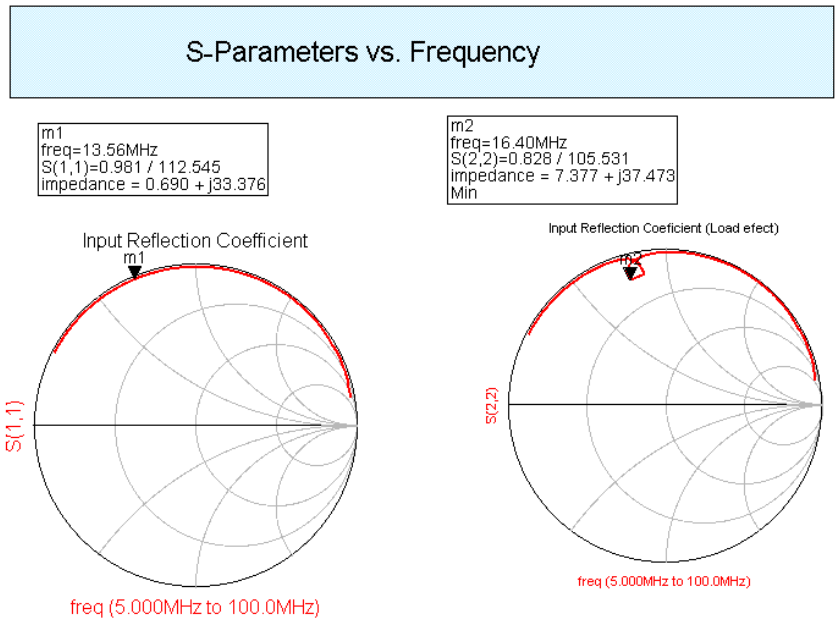


Fig. 53) Bobina 2 espiras em PCB. a) sem o efeito carga; b) com efeito carga

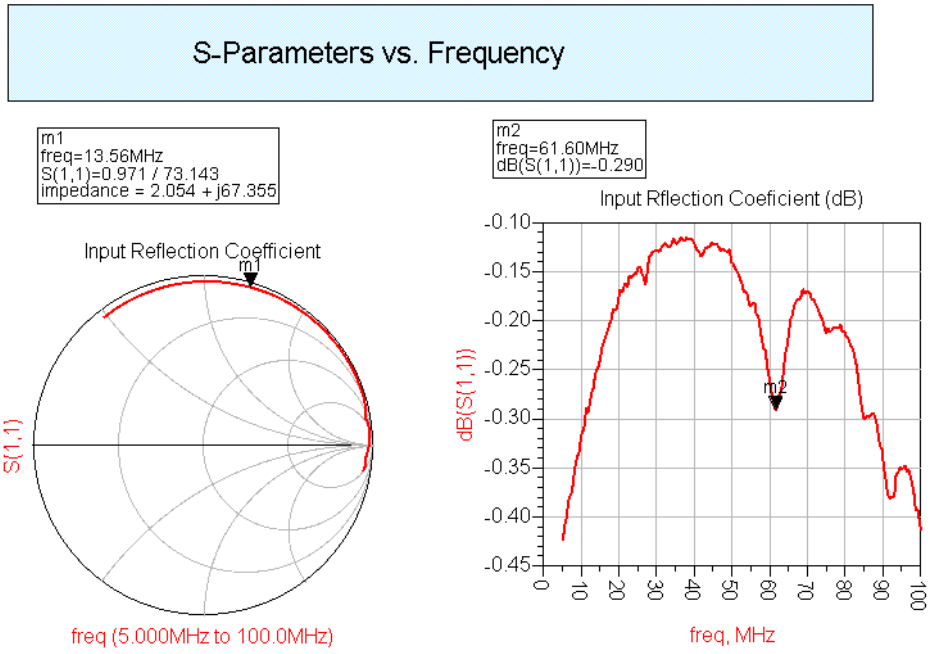


Fig. 54) Bobina 3 espiras em PCB sem efeito de carga

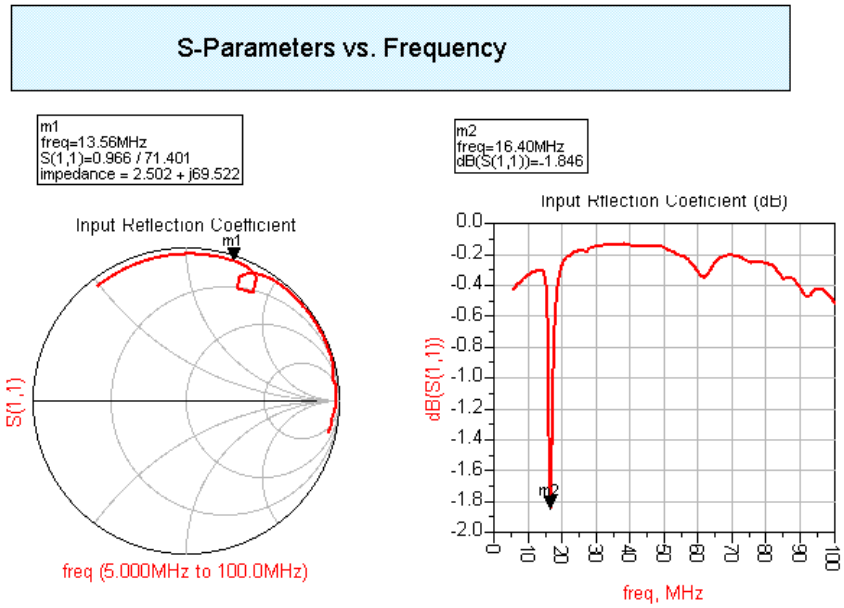


Fig. 55) Bobina 3 espiras em PCB com efeito de carga

5.2 – Sinais de interface RF

Nesta secção pretende-se verificar a conformidade dos sinais de interface RF com a parte 2 do standard ISO14443. A metodologia seguida consistiu em curto-circuitar a ponta de prova do osciloscópio/analisador de espectro sobre si mesma de modo a operar como uma antena indutiva (bobina) e interpô-la entre o leitor e o transponder conforme mostrado na figura seguinte. Deste modo a pôde-se analisar os sinais na interface rádio.

Fig. 56) *Setup* utilizado

As figuras 55, 56 e 57 mostram os espectros de sinal numa transacção ISO14443A. O sinal é mostrado no domínio temporal (à esquerda) e na frequência (à direita). A Fig. 55 mostra a primeira fase da comunicação na qual o leitor faz a difusão da portadora que irá alimentar

os transponders no campo de leitura. A risca central no gráfico da direita representa a portadora (13.56MHz).

A Fig. 56 mostra a operação de *downlink*, envio de comandos/dados ao transponder. A portadora é modulada em amplitude com dados a um ritmo $R_{TX} = f_c/128 = 105.9375$ kbps (ritmo de transmissão de dados utilizado na arquitectura Mifare) com codificação Miller modificado. Na Fig. 57 pode-se ver a modulação de carga com codificação Manchester produzida pelo transponder. Nos sistemas indutivos passivos, a resposta do transponder é extremamente fraca, como se pode ver pela figura (mais de 60 dBs abaixo da portadora), razão pela qual é necessária uma técnica de modulação robusta para que o leitor possa detectar a informação enviada pelo transponder. Deste modo, utiliza-se em *uplink* uma sub-portadora à frequência $f_s = f_c / 16 = 847.5$ kHz. Isto resulta, como se pode ver no gráfico da direita, num deslocamento do espectro banda-base ($R_{TX} = 105.9375$ kHz) que passa a estar centrado em $f_o = f_c \pm f_s = 13.56$ MHz ± 0.8475 MHz = 14.4075 e 12.7125 MHz. A sub-portadora é modulada, à semelhança da operação de *downlink*, com dados a um ritmo R_{TX} = 105.9375 kHz. A sub-modulação confere maior robustez à operação de *uplink*, que fica assim mais imune a possíveis interferências externas e facilita a detecção da informação no leitor.

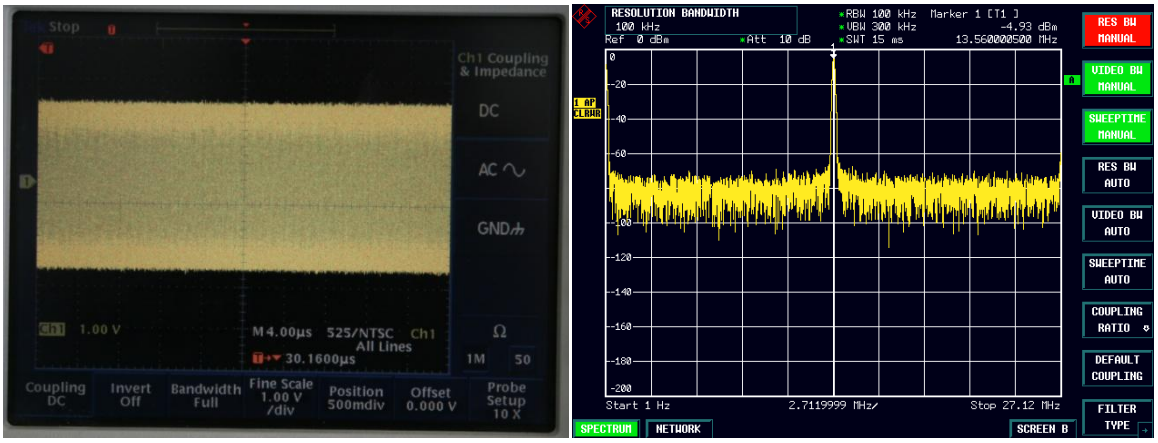


Fig. 57) Portadora sem modulação (leitor). a) Domínio temporal; b) Frequência

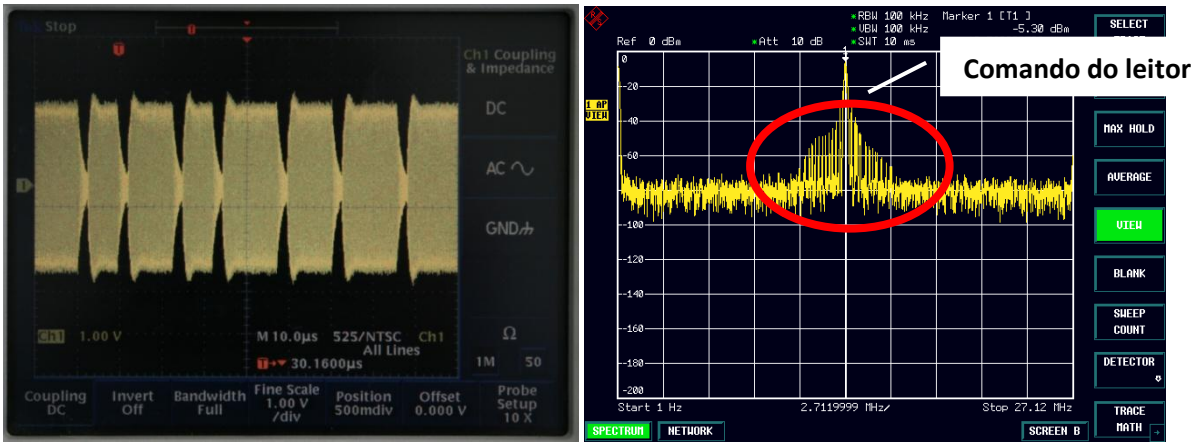


Fig. 58) Portadora modulada (leitor). a) Domínio temporal; b) Frequência

Fig. 59) Modulação de carga (tag). a) Domínio temporal; b) Frequência

5.3 – Efeito de diversos materiais no alcance de leitura

Nesta secção pretende-se avaliar o efeito de diversos materiais no alcance de leitura. Para isso vai-se interpor entre o leitor e o transponder diversos materiais como papel, cartão, plástico (saco), plástico rígido, PCB, metal, carteira (cabedal), ganga e tecido e analisar o efeito. A tabela seguinte mostra os resultados obtidos.

Material na linha de vista	**Alcance (cm)**	**Comentários**
----------	7.4	Sem obstáculos
Papel	6.9	
Cartão	5.5	
Saco plástico	7.2	
Plástico rígido	5.1	
Cabedal (carteira)	6.7	Pouco efeito
Carteira com moedas	6.6	
Ganga	7.3	Pouco efeito
Tecido (pano)	7.3	
PCB	1.4	Bloqueio parcial
Chapa de metal	----------	Bloqueio total

Tabela 7) Alcance do leitor

Como seria de esperar, a chapa de metal entre o leitor e o transponder bloqueia completamente a comunicação. Com o PCB, ainda que a uma distância curta, consegue-se uma leitura a 1.4 cm. O cartão e o plástico rígido provocam uma diminuição significativa do alcance de leitura, enquanto o cabedal, a ganga e o tecido pouco interferem na distância de leitura.

Capítulo 6 – Conclusões

A tecnologia RFID ganha cada vez mais afirmação no mercado mundial e está presente no nosso quotidiano. No entanto, surgem novos desafios como o da procura de soluções l*ow cost* que permitam massificar o uso da tecnologia. Existe actualmente, no mercado, um conjunto de soluções integradas capazes de implementar diversos protocolos. Um exemplo é o transceiver HF RFID utilizado neste projecto.
Neste trabalho, propôs-se o desenvolvimento de uma solução RFID vendável para a banda ISM HF (13.56 MHz). Para tal, primeiramente foi necessário escolher o standard sobre o qual se iria trabalhar bem como os transponders a utilizar de acordo com as necessidades reais. A escolha dos transponders recaiu sobre a família de cartões de proximidade da NXP, compatíveis com o standard ISO14443-A. Esta escolha, como já foi referido atrás, deveu-se ao facto da NXP ser actualmente um dos maiores fabricantes mundiais de cartões sem contacto. Para o desenvolvimento do leitor recorreu-se a um transceiver RFID HF, também da NXP, o transceiver MFRC531 que constituiu o *core* do leitor.
Pensa-se que os objectivos propostos foram alcançados com êxito. Graças ao levantamento do estado da arte adquiriu-se um conhecimento considerável da arquitectura e princípio de funcionamento dos sistemas RFID actuais, com ênfase nos sistemas indutivos de proximidade. O *know how* adquirido no desenvolvimento/integração do 1º protótipo do leitor serviu de base à construção de uma versão final, comercializável, que será brevemente colocada no mercado pela Acronym.
A maior dificuldade encontrada na realização prática do trabalho prende-se com a implementação do protocolo ISO14443-A. Há algumas situações menos explícitas no protocolo que levam a interpretações ambíguas. Esta dificuldade foi contornada com um desenvolvimento sistemático do firmware. Procurou-se tanto quanto possível testar e verificar a coerência dos resultados obtidos em todas as etapas da implementação.
Do ponto de vista empresarial, a principal mais-valia deste trabalho foi conseguir-se desenvolver um produto final, acabado e vendável.

6.1 – Trabalho futuro

Este projecto deixou portas abertas a trabalhos de continuidade e trouxe novas ideias e perspectivas de trabalho futuro:

- O transceiver utilizado neste projecto permite também a implementação do protocolo ISO14443-Tipo B. Um trabalho complementar seria portanto implementar este protocolo, conferindo ao leitor uma maior multifuncionalidade.

- O leitor desenvolvido permite um alcance de leitura de 7-8 cm sem amplificação externa. Existe a possibilidade de incorporar um *font-end* para melhorar o alcance.
- Neste projecto não se implementou o mecanismo anti-colisão, por se considerar que com o alcance actual (7-8cm) é improvável a presença simultânea de cartões no campo do leitor. Com a construção do *front-end* referido no ponto anterior, um outro trabalho de continuidade seria a anti-colisão.
- Finalmente apresenta-se uma proposta alternativa para construção do leitor que surgiu no decorrer deste trabalho (sugestão do orientador). Com o novo paradigma de rádio por software (SDR – Software Defined Radio), muitas das tarefas antes realizadas pelo hardware passam agora a ser realizadas inteiramente por software. A proposta aqui apresentada, vai no sentido de se implementar todas as camadas do protocolo ISO14443-A ou outro em software. Assim sendo, à semelhança do processamento banda-base, também a codificação e a modulação seriam feitas em software, dispensando a utilização do transceiver. O leitor passaria a ser constituído apenas pelo MCU, um *front-end* e uma antena. Para sistemas LF (125kHz) e HF (13.56MHz), bastaria um microprocessador idêntico ao utilizado neste projecto para se conseguir "sintetizar" e processar o sinal RF. No caso de um sistema UHF, seria necessária uma etapa de conversão intermédia (*downconverter/upconverter*) e eventualmente uma DSP.

Referências Bibliográficas

1. http://www.gemalto.com/php/pr_view.php?id=491 . [Online] [Citação: 19 de Maio de 2009.]

2. **Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia.** *"A Practical Attack on the MIFARE Classic".*

3. http://pt.wikipedia.org/wiki/RFID. [Online] [Citação: 21 de Maio de 2009.]

4. http://www.portalrfid.net/. [Online] [Citação: 21 de Maio de 2009.]

5. **Finkenzeller, Klaus.** *"RFID Handbook, 2nd Edition ed. Wiley".*

6. **Gomes, Hugo Miguel Cravo.** *"Construção de um sistema de RFID com fins de localização especiais".* 2007.

7. **Stockman, Harry.** *"Communication by Means of Reflected Power, Proceedings of theIRE, pp 1196-1204".* October 1948.

8. http://www.rfidconsultation.eu/docs/ficheiros/shrouds_of_time.pdf. [Online] [Citação: 21 de Maio de 2009.]

9. **Philips and German Public Transport Network Operator RMV trial NFC for ticketing, Nokia.** http://press.nokia.com/PR/200411/966921_5.html. [Online] [Citação: 22 de Maio de 2009.]

10. **I-Code, NXP semiconductors.** http://www.nxp.com/#/pip/pip=[pfp=42024]|pp=[t=pfp,i=42024]|. [Online] [Citação: 21 de Maio de 2009.]

11. **Bob Scher, CEO Dynasys Technologies, Inc.** *"Transponder Types".*

12. **Alien, Technology.** *"RFID Primer, All Readers".*

13. http://rfid-handbook.de/rfid/frequencies.html. [Online] [Citação: 2009 de Maio de 5.]

14. **Pereira, Alessandro de Souza Oliveira e Milene Franco.** *"Estudo da tecnologia de identificação por radiofrequência".* 2006.

15. **ISO, International Organization For Standardization.** http://www.iso.org. [Online] [Citação: 2009 de Maio de 6.]

16. **ISO/IEC.** *" Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 1: Physical characteristics ".* 2007.

17. —. *"Identification cards — Contactless integrated circuit(s) cards - Proximity cards — Part 3: Initialization and anticollision".* 2007.

18. **Inc., EPCGlobal.** http://www.epcglobalinc.org. [Online] [Citação: 7 de Maio de 2009.]

19. 8-bit AVR Microcontroller - ATMega16 Datasheet.

20. **Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia.** *"A Practical Attack on the MIFARE Classic".*

21. **semiconductors, NXP.** *"Datasheet transceiver MFRC531".*

22. **Semiconductors, NXP.** *"MF1CS70 , Functional specification Rev.4.1".* 2008.

23. —. *"MF1CS50 , Mifare Standad Card Datasheet".*

24. http://www.nxp.com/acrobat_download/other/icode_supplier_list_2008_10.pdf. [Online]

25. **ISO/IEC.** *" Identification cards – Contactless integrated circuit(s) cards – Proximity cards – Part 2: Radio frequency power and signal interface ".* 2007.

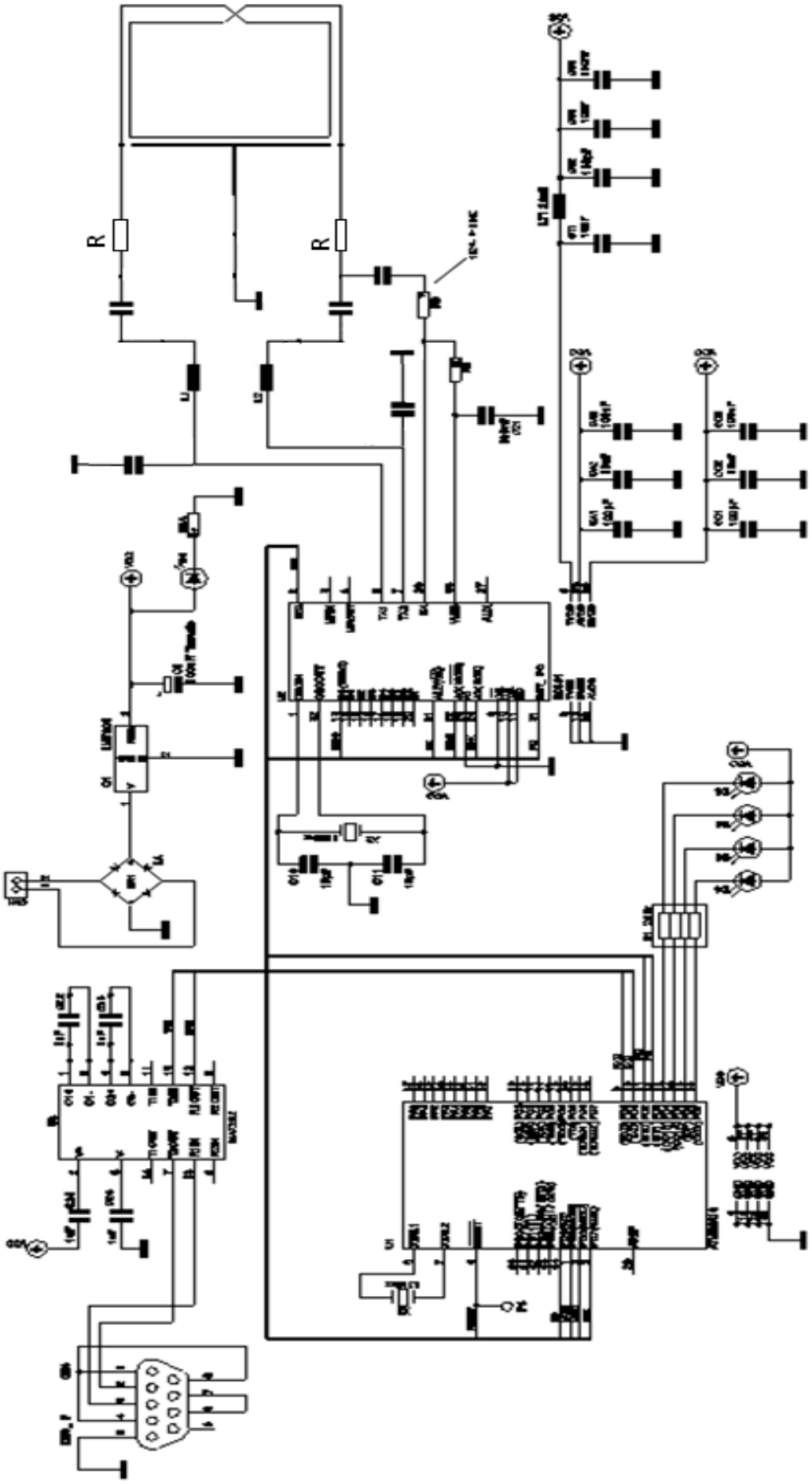
26. —. *"Identification cards — Contactless integrated circuit(s) cards - Proximitycards — Part 3: Initialization and anticollision".* 2007.

27. —. *"Identification cards — Contactless integrated circuit(s) cards —Proximity cards — Part 4: Transmission protocol".* 2007.

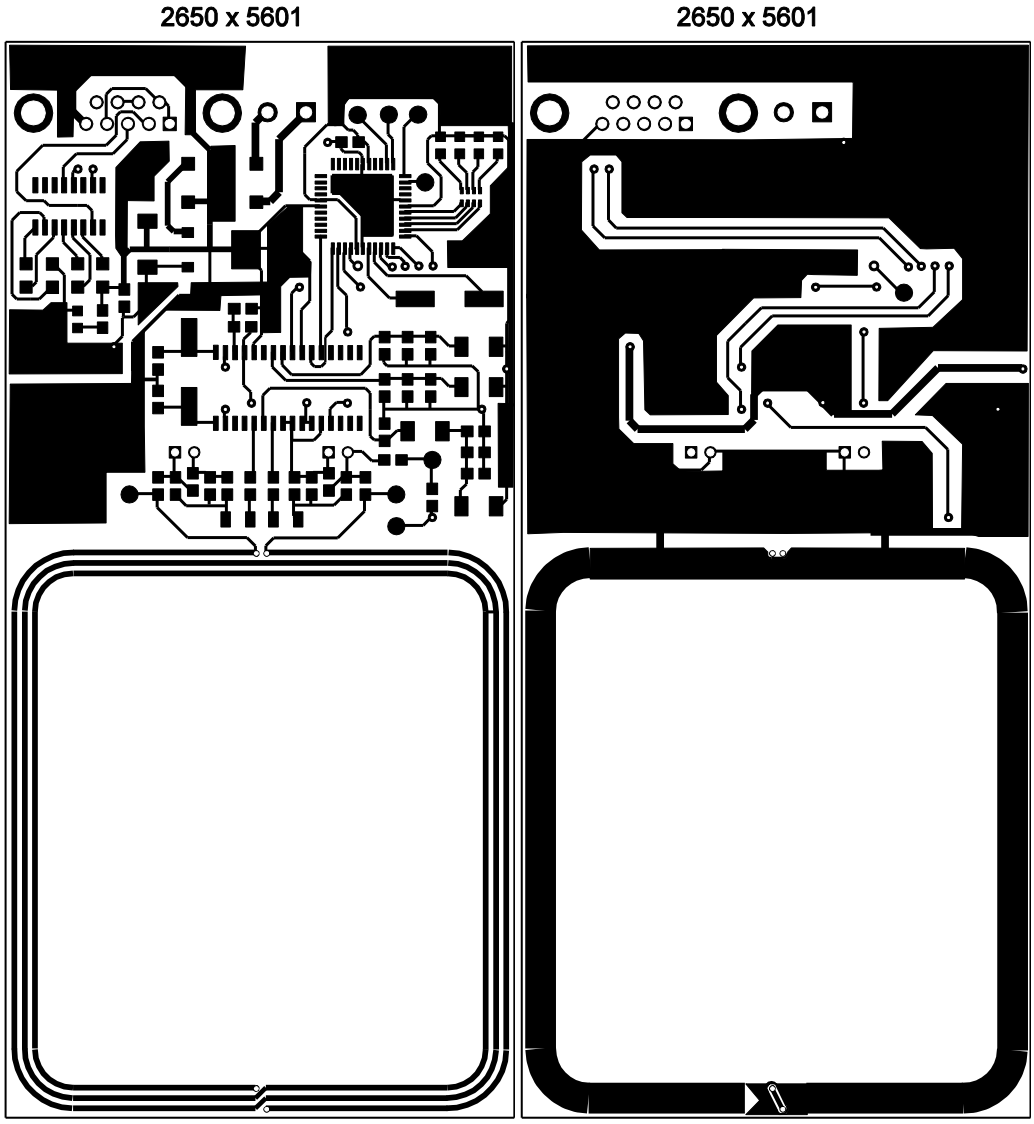
28 – **Sedra And Smith** "Microelectronic Circuits", 4ª Ed.

29 – **José Carlos Pedro** "Apontamentos de Electrónica de Rádio Frequência"

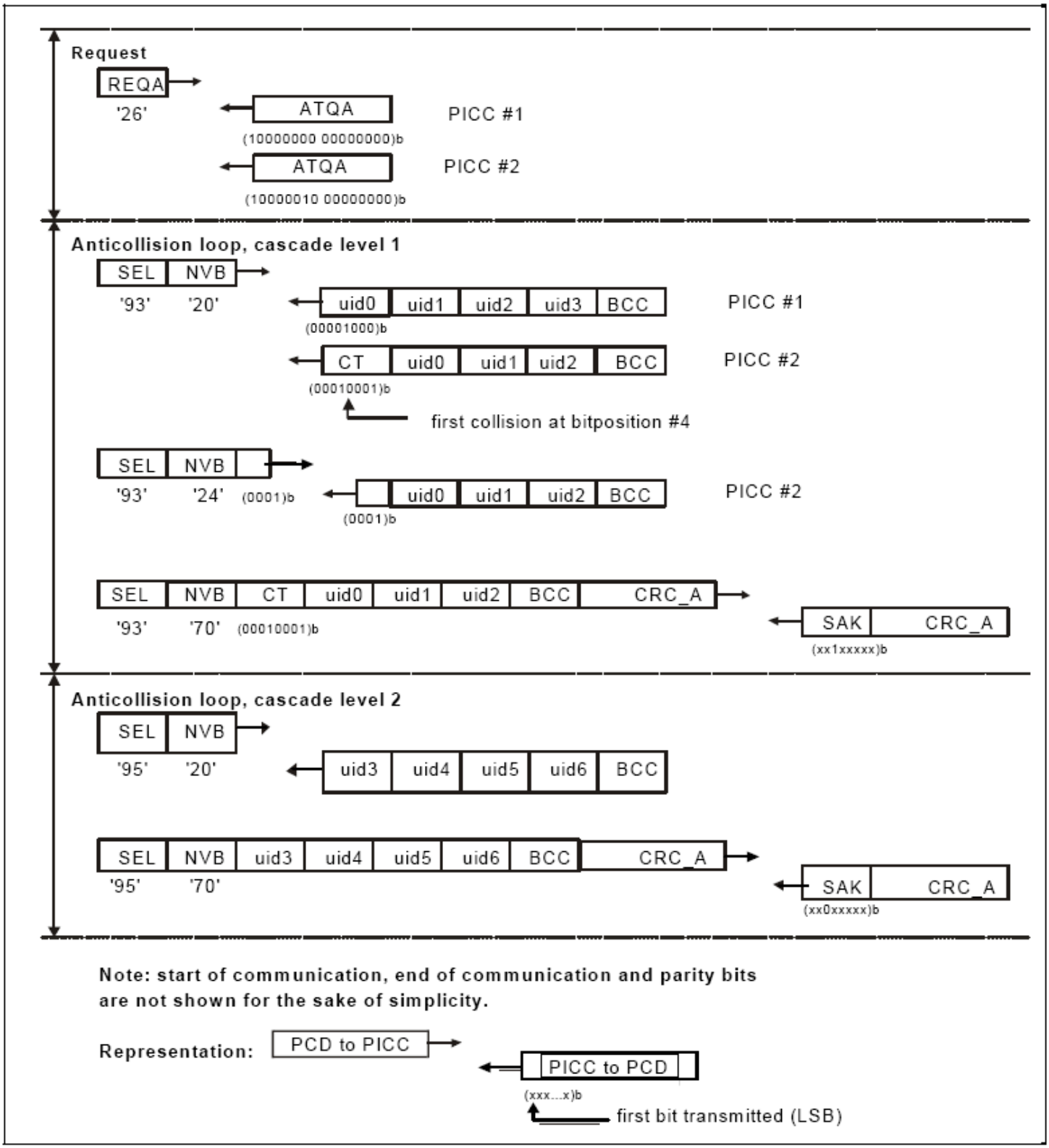
ANEXO 1) Esquema eléctrico do leitor



ANEXO 2) Layout (Top e Bottom) do circuito impresso



ANEXO 3) Mecanismo de anti-colisão ISO14443-A, dois transponders no campo



ANEXO 4) Código desenvolvido

Estrutura de dados global:

```
typedef struct
      {

        unsigned char  cmd;                // Código Hexadecimal do comando executar  no transceiver
        char           status;             // Estado do comunicação : 0-CmdOngoing; 1-CmdDone
        unsigned short nBytesToSend;       // Número de bytes a enviar ao tag
        unsigned short nBytesReceived;     //Número de bytes recebidos do tag
        unsigned long  nBitsReceived;      // Número de bits recebidos do tag
        unsigned char  irqSource;          // Interrupções ocorridas durante a execução do comando
        unsigned char  collPos;            // Posição de colisão, útil para resolver colisões
        unsigned char  errFlags;           // Erros ocorridos durante a execução do comando

         } INFO;
```

INFO CMDInfo;

Buffer global:

```
#define MEMORY_BUFFER_SIZE    64
unsigned char SENDERBuffer [MEMORY_BUFFER_SIZE];        // Buffer para envio de dados ao tag
unsigned char RECEIVERBuffer [MEMORY_BUFFER_SIZE];      // Buffer de recepção de dados do tag
```

Main:

```
{
        // Leitura de 16 bytes da memória do transponder (bloco 1)
        SENDERBuffer [0] = PICC_READ16;                 // Código do comando read
        SENDERBuffer [1] = block_addr=1;                // Endereço do bloco a ler
        CMDInfo.nBytesToSend   = 2;                     // Número de Bytes a enviar a tag
        status = PCDCmdRequest(PCD_TRANSCEIVE);          // Execução do commando tranceive

        return status;
}
```

PCDCmdRequest :

```
signed char PCDCmdRequest(unsigned char cmd)
{
        unsigned char i;
        signed char status;
        status = MI_OK;

        CMDInfo.cmd=cmd;
        CMDInfo.status=CMD_ONGOING;

        ISR_conf();                                     // Configuração das interrupções

        switch (cmd)
        {
```

```
                case PCD_TRANSCEIVE:

                        FlushFIFO();                                    // Assegurar que o FIFO está vázio
                        for(i=0;i<CMDInfo.nBytesToSend;i++)     //Escrever os dados a enviar no buffer
                                WriteReg(RegFIFOData,
SENDERBuffer[i]);WriteReg(RegInterruptEn,0xa8);          //Ligar as interrupções necessárias: Rx e Tmr

                        break;


                case PCD_LOADKEY:

                        FlushFIFO ();
……
……
……
        }

        WriteReg(RegCommand,CMDInfo.cmd);               // Executar o commando no
transceiverwhile(CMDInfo.status!=CMD_DONE);              // Aguardar que o comando seja executado no
nível hardware

        WriteReg(RegCommand,PCD_IDLE);                  // fazer reset ao registo comando
        // Avaliar os erros e devolvê-los a função invocadora

        return status;


}
```

Rotina de Serviço a Interrupção:

```
ISR (INT0_vect)
{
        char cSREG,i,aux;

                cSREG=SREG;                     // Salvaguardar o registo status do uP

                switch (CMDInfo.cmd)
                {
                case PCD_TRANSCEIVE:

                        // Fazer o Update da estrutura de dados  global (Errors, status...)
                        CMDInfo.nBytesReceived=ReadReg(RegFIFOLength);      // Bytes recebidos

                        CMDInfo.nBitsReceived=8*CMDInfo.nBytesReceived;     // Bits recebidos

                        //Fazer o  Update do buffer  global de dados

                for(i=0;i<CMDInfo.nBytesReceived;i++)    //Ler dados do FIFO
                                RECEIVERBuffer [i]=ReadReg(RegFIFOData);

                        break;
                case PCD_LOADKEY:
                        StopTimerNow();
```

```
                ……..
        ……….

                }

                CMDInfo.irqSource=ReadReg(RegInterruptRq);      // Ler registo de interrupções
                CMDInfo.errFlags=ReadReg(RegErrorFlag);          // Ler registos de erro

                WriteReg(RegInterruptRq,0x3f);                  // Desactivar  interrupt request
                WriteReg(RegInterruptEn,0x7F);                  // Desactivar interrupt
                CMDInfo.status=CMD_DONE;    // Comunicar ao nível superior a conclusão do comando

                SREG=cSREG;                                     // Restaurar o registo status do CPU
}
```

```
signed char RequestAll(unsigned char req_code, unsigned char *atq)
{
        signed char status = MI_OK;
         Set_timer(60);                                  //Numero de ETUs  =60 -> TimeOut=564us;
        WriteReg(RegChannelRedundancy,0x03);            // RxCRC e TxCRC activos, paridade inactiva
        ClearBitMask(RegControl,0x08);                   // crypto 1 inactivo
        WriteReg(RegBitFraming,0x07);                    // TxLastBits = 7

         ResetInfo(CMDInfo);
          SENDERBuffer[0] = req_code;
         CMDInfo.nBytesToSend  = 1;
         status = PCDCmdRequest(PCD_TRANSCEIVE);
        // Avaliação de erros ocorridos
        if ((status == MI_OK) && (CMDInfo.nBitsReceived != 16))  // 2 bytes Esperados (ATQA)
        {       status = MI_BITCOUNTERR;
        }
        if (CMDInfo.nBytesReceived = 2) {
        memcpy(atq,RECEIVERBuffer,2);
         }
        else {
        atq[0] = 0x00;
         atq[1] = 0x00;
        }
          return status;
}
```

```
signed char MultiLevelAnticoll(unsigned char cascad_anticol, unsigned char *snr)
{
        signed char status;
        unsigned char coll_pos;    // Posição da primeira colisão ocorrida na interface RF
        unsigned char nvb;         // Numero de bites válidos (MSShort-numero de bytes; LSShort-numero
de bits)
        status = MI_OK;
        Set_timer(100);                         // Prevenir timeout na interface ar
```

```
        ClearBitMask(RegControl,0x08);          // desactivar crypto 1
        ResetInfo(CMDInfo);                     // Reset da estrutura global de controlo
        WriteReg(RegChannelRedundancy,0x03);    // RxCRC e TxCRC inactivos, paridade activa
                ///////////////// 1ª Parte da anticolisão – envio de 2 bytes ////////////////
        SENDERBuffer[0] = cascad_anticol;
        nvb=0x20;
        SENDERBuffer[1] = nvb;
        CMDInfo.nBytesToSend   = 2;
        status = PCDCmdRequest(PCD_TRANSCEIVE);
        if(status==MI_COLLERR)                  // Se colisão todos os tags são postos em estado Idle
                 Halt_Card();
        else
                memcpy(snr,RECEIVERBuffer,4);
        // A fazer .....
                /*///////////////// Anticollision Loop ////////////////////////
        return status;
}


signed char MultiLevelSelect(unsigned char select_code, unsigned char *snr, unsigned char *ats)
{
          signed char   status = MI_OK;
   Set_timer(100);                              // Prevenir Timout na interface RF
   WriteReg(RegChannelRedundancy,0x0F);         // RxCRC,TxCRC e Paridade activos
   ClearBitMask(RegControl,0x08);               //desactivar crypto 1
   // Preencher buffer de dados global
   ResetInfo(CMDInfo);
   SENDERBuffer[0] = select_code;               // nível cascade
   SENDERBuffer[1] = 0x70;                      // NVB número de bytes válidos a enviar: 7 bytes
    memcpy(SENDERBuffer + 2,snr,4);
   //Cálculo do BCC1: Exclusive-Or dos 4 Bytes do UID
   SENDERBuffer[6] = SENDERBuffer[2]^ SENDERBuffer[3]^ SENDERBuffer[4]^ SENDERBuffer[5];
   CMDInfo.nBytesToSend   = 7;
   status = PCDCmdRequest(PCD_TRANSCEIVE);
   if (status == MI_OK)
   {
     if (CMDInfo.nBitsReceived != 8)            // Ultimo byte incompleto
    {        status = MI_BITCOUNTERR;
     }
     else       {
       memcpy(SelectedUID,snr,4);
     }
   }
  return status;
}


signed char ReadPICCDataBlock( unsigned char addr, unsigned char *data)
{
  signed char status = MI_OK;
  char bitsExpected;
  int i;
  unsigned char datalen=16;
```

```
  Set_timer(700);  // timeout longo
  WriteReg(RegChannelRedundancy,0x0F); // RxCRC, TxCRC e paridade activos
          // Sequência de comandos: Enviar commando Read e endereço a ler  e esperar  AK/NAK
  ResetInfo(CMDInfo);
  SENDERBuffer[0] = PICC_READ16;   // commando read
  SENDERBuffer[1] = addr;
  CMDInfo.nBytesToSend   = 2;
  status = PCDCmdRequest(PCD_TRANSCEIVE);
  if(status==MI_OK)
  {
    if (CMDInfo.nBytesReceived != datalen)      {
      status = MI_BYTECOUNTERR;
     }
    else  {
      memcpy(data,RECEIVERBuffer,datalen);
    }
  }
  else
                      status=MI_READERR;
  return status;
}
```