UNIVERSIDADE DA BEIRA INTERIOR

Engenharia

Estudo do potencial de aplicabilidade da tecnologia RFID em meio hospitalar

Idália Sofia Gouveia Pedro

Dissertação para obtenção do Grau de Mestre em:

Engenharia Electrotécnica e de computadores

(2º ciclo de estudos)

Orientador: Prof. Doutor António Eduardo Vitória do Espírito Santo

Covilhã, Outubro de 2012

Agradecimentos:

Antes de mais quero agradecer ao meu orientador, o Professor Doutor António Eduardo Vitoria do Espírito Santo por me ter sempre guiado neste trabalho com muita sabedoria e paciência, pela sua grande ajuda e disponibilidade.

Aos meus pais e as minhas irmãs que mesmo estando longe sempre me fizeram sentir o seu carinho e apoio.

Ao meu namorado Nelson Mendes pela motivação, companheirismo e apoio incondicional que sempre demonstrou.

Aos restantes amigos pela vossa amizade e por acreditarem sempre em mim.

Ao pessoal do laboratório pela amizade e apoio nos últimos meses desta dissertação.

A todos vos, o meu muito obrigado, pois de uma maneira ou de outra fizeram um marco na minha vida e contribuíram de alguma maneira na pessoa que sou hoje.

Resumo

A identificação por radiofrequência (RFID) é uma tecnologia que já existe há umas décadas. Porém, só há uma dezena de anos, é que esta tem vindo a ter uma utilização crescente. A tecnologia RFID é apontada como sendo o futuro da tecnologia da identificação automática, sendo que já é um sucesso na área da gestão de cadeias fornecimento de produtos.

Estudos científicos afirmam que esta tecnologia é muito versátil oferecendo um grande leque de aplicabilidade em diversas áreas, afirmando que no sector hospitalar, a implementação de sistemas RFID apresenta grandes vantagens podendo mesmo revolucionar os cuidados médicos.

Esta dissertação tem como principal objectivo perceber se a implementação desta tecnologia em meio hospitalar representa realmente uma mais-valia. Desta feita, pretende-se discutir as suas vantagens e as desvantagens. Em paralelo são apresentadas e discutidas aplicações numa área tão complexa como a da saúde. Para isso, são estudados os componentes desta tecnologia, os diferentes modos destes interagirem e as suas diversas funcionalidades. Com o intuito de abordar a identificação de radiofrequência, de um ponto de vista mais prático, testou-se o funcionamento do módulo TRF760EVM da Texas Instrument. Dada a complexidade e as exigências do meio hospitalar analisou-se os efeitos do campo electromagnético dos sistemas RFID sobre o corpo humano e equipamento médico.

Palavras-chaves

Identificação por radiofrequência (RFID), etiqueta, leitor, sistemas activos/passivos, meio hospitalar, segurança, privacidade, interferências electromagnéticas, compatibilidade electromagnética

Abstract:

The radio frequency identification (RFID) is a technology that has existed for a few decades, however only in the last decade that it has been a growing technology. RFID is being pointed as the future of automatic identification technology, and is already a success in the area of supply chain management products.

Scientific studies say that this technology is a very versatile offering for a wide range of applicability in several areas. Whereas in the healthcare sector, the implementation of RFID systems represents great advantages and may even revolutionize healthcare.

This work main objective's, is analyzing the benefits and drawbacks of RFID, realizing if the implementation of this technology in a hospital is really an asset. For this, the first step is to study the components of this technology and the different way as they interact and their various features. With the intention of addressing the radio frequency identification from a more practical point of view, we tested the operation of the module TRF760EVM from Texas Instrument. Next, we investigated the possibilities of applications in hospitals and some existing products for these uses. Since this environment is complex, we analyzed the effects of the electromagnetic field of RFID systems over the human body and surrounding medical facilities.

Keywords

Radiofrequency identification (RFID), tag, reader, active/ passive system hospital facilities, security, privacy, electromagnetic interferences, electromagnetic compatibility

Índice

Lista de Figuras

Lista de Tabelas

Lista de acrónimos:

RFID	Radio Frequency Identification
EAN	European Article Number
JAN	Japanese Article Numbering
UPC	Universal Product Code
ADC	Analogue-to-Digital Converter
LPF	Low-Pass Filter
IFF	Identifier Friend or Foe
EAS	Electronic Article Surveillance
CMOS	Complementary Metal-Oxide Semiconductor
EEPROM	Electrically-Erasable Programmable Read-Only Memory
EPC	Electronic Product Code
ISO	International Organization for Standardization
AC	Alternating Current
LF	Low-Frequency
HF	High-Frequency
UHF	Ultra High-Frequency
RF	Radiofrequência
DAC	Digital-to Analogue Converter
ID	Identificação
IC	Integrated Circuit
ASIC	Application-Specific Integrated Circuit

RO	Read Only
WORM	Write Once- Read Many
RW	Read/ Write
DSP	Digital Signal Processor
RAM	Random Access Memory
ROM	Read-Only Memory
µP	Microprocessador
ASK	Amplitude Shift Keying
BSK	Bi-Phase Shift Keying
EPCIS	Electronic Product Code Information Service
ONS	Object Name Serving
AES	Advanced Encryption Standard
CLK	Clock
Reg.	Remote Administration Control
Rcon.	Remote Administration Control
SDMA	Space-Division Multiple Access
FDMA	Frequency- Division Multiple Access
CDMA	Code-Division Multiple Access
TDMA	Time-Division Multiple Access
UID	Unique Identification
TTF	Tag-Talk-First
RTF	Reader-Talk- First
SA	Slotted Aloha

FSA	Framed Slotted Aloha
BFSA	Basic Framed Slotted Aloha
DFSA	Dynamic Framed Slotted Aloha
PA	Pure Aloha
REV	Revision
USB	Universal Serial Bus
LED	Light-Emitting Diode
SPI	Serial Peripheral Interface
PCB	Printed Circuit Board
JTAG	Join Test Action Group
RSSI	Received Signal Strength Indicator
AM	Amplitude Modulation
PM	Phase Modulation
AGC	Automatic Gain Control
SOF	Start Of Frame
IEC	International Electrotechnical Commission
AFI	Application Family Identifier
DSFID	Data Storage Format Identification
OEM	Original Equipment Manufactures
UART	Universal Asynchronous Receiver/ Transmitter
I2C	Eye-two-Cee
GPIO	General Purpose Input/Output
RSTL	Real-Time Location System

VDC	Volts of Direct Current
IS-RFID	Inpatient Safety RFID System
PRNG	Pseudo-Random Number Generator
SIH	Sistema de Informação do Hospital
EN	European Standards
SAR	Specific Absorption Rate
FCC	Federal Communications Commission
EMI	Electromagnetic Interferences
ANSI	American National Standards Institute
EMC	Electromagnetic Compatibility

1. Identificação automática

Nos últimos anos, os sistemas automáticos de identificação têm vindo a ter uma aplicabilidade cada vez maior nos mais diversos sectores de actividade, nomeadamente, na monitorização de bens ou na gestão do fluxo de produtos. As tecnologias de identificação automática são, geralmente, utilizadas na recolha de informação sobre pessoas, animais ou produtos em trânsito [1].

Existem várias alternativas tecnológicas que tornam possível a identificação automática. Temos, por exemplo, a identificação biométrica que permite a identificação por voz, a leitura de impressões digitais, ou a leitura da íris. Outro exemplo é o reconhecimento de caracteres ópticos que reconhece e transforma caracteres em textos legíveis. As tecnologias envolvidas quer na biometria quer no reconhecimento óptico de caracteres são seguras, no entanto, o preço deste tipo de equipamento é bastante elevado e, por si só, não proporciona qualquer meio de rastreio. Outra alternativa possível é a tecnologia associada às etiquetas de códigos de barras. Esta solução, para além de apresentar um preço baixo, permite também uma fácil utilização. Esta Dissertação de Mestrado debruça-se sobre a tecnologia de *Radio frequency Identification* (RFID), ou, em português, Identificação por Radiofrequência. Esta tecnologia recorre às ondas de rádio para comunicar com etiquetas que podem custar desde alguns cêntimos a uma centena de euros, consoante a aplicação e as características desejadas. Contudo, até as etiquetas mais baratas conferem um meio de identificação único e seguro, permitindo desta forma a implementação de sistemas de rastreabilidade [2].

1.1. Sistema de código de barras

Os códigos de barras são uma tecnologia de identificação que se baseia em conceitos de óptica, electrónica, comunicação e tecnologias da computação. As etiquetas de códigos de barras, que suportam a informação a codificar, são compostas por barras (bandas pretas) e espaços (bandas brancas) [3]. A sua construção obedece a regras de codificação estabelecidas através de normas internacionais, sendo que existem três organismos responsáveis pela normalização desta tecnologia: *European Article Number* (EAN), *Japanese Article Numbering* (JAN) e a *Universal Product Code* (UPC) [4].

Na figura 1, mais abaixo, podemos encontrar dois códigos de barras retirados de duas embalagens de medicamentos diferentes. Assim, olhando para os dois códigos de barras, podemos observar que são compostos por uma combinação de bandas pretas e brancas, de espessuras variáveis.

Um leitor de código de barras é utilizado para ler estas etiquetas. O leitor emite um feixe de luz que varre toda a etiqueta, sendo que, nos sítios onde se encontram as bandas pretas a luz é absorvida e onde existem bandas brancas esta é reflectida de volta ao leitor. Existem diversos tipos de leitores, tais como, por exemplo: leitores de espelhos, leitores holográficos e leitores electromagnéticos de polímeros.

Na figura 2 podemos encontrar um diagrama de blocos descritivo da constituição de um leitor electromagnético de polímeros. No início do processo, uma linha de luz varre o código de barras, sendo que um fotodíodo vai receber a luz reflectida pelo código de barras (ver figura 3). O sinal óptico recebido é amplificado e convertido em tensão por um amplificador de transimpedância. Após essa etapa, um diferenciador calcula a taxa de variação do sinal em relação ao tempo. Na prática, vamos obter uma variação consoante o feixe de luz atravessa uma banda preta ou branca. De seguida, o sinal vai ser convertido para o domínio digital por um *Analogue-to-digital Converter* (ADC) com 10-bits de resolução para que um microcontrolador possa descodificar o sinal [5].

a b

Figura 1: Código de barras pertencendo a duas caixas de medicamentos.

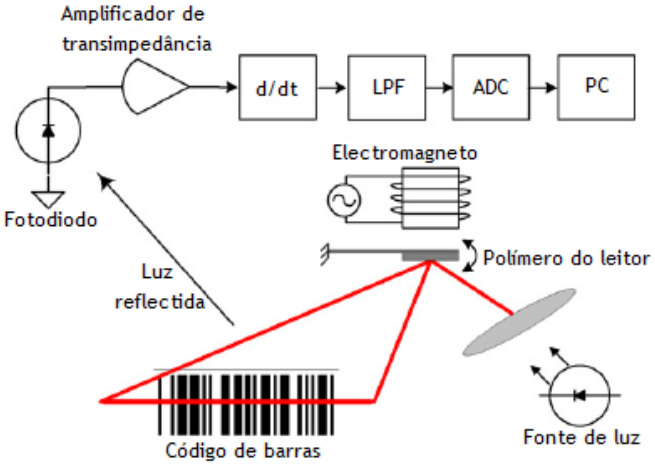


Figura 2: Diagrama de blocos de um leitor de código de barras [5].

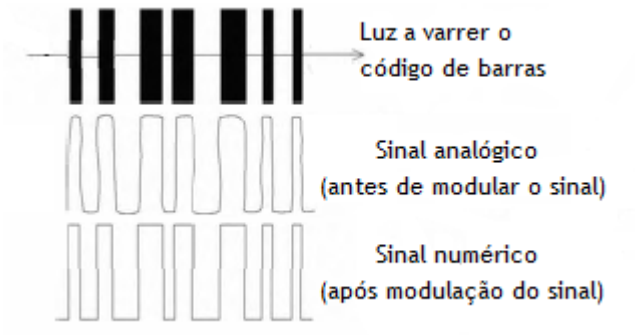


Figura 3: Esquema representativo das modificações do sinal ao longo do seu processamento [3].

1.2. Sistema de identificação por radiofrequência (RFID)

Contrariamente aos sistemas de código de barras, no que toca à identificação por radiofrequência (RFID), a comunicação e transmissão dos dados entre o leitor e as etiquetas é realizada através de ondas electromagnéticas. Esta tecnologia permite, assim, a identificação e a transmissão de dados sem que haja necessidade de haver contacto directo entre o leitor e as etiquetas (ou *tags*). A operação de comunicação pode mesmo ocorrer sem necessidade de intervenção de mão humana. Os factos identificados anteriormente apresentam-se como mais-valias relativamente ao código de barras [6].

Na tabela 1, encontram-se resumidas as grandes diferenças entre a tecnologia RFID e a tecnologia de código de barras. Da sua consulta podemos concluir que a tecnologia RFID é mais eficiente e versátil [7].

Os sistemas RFID são constituídos por quatro componentes principais, a saber: o leitor, as etiquetas, as antenas e o software de gestão das diferentes funcionalidades. De um modo simplificado, o sistema pode funcionar de duas maneiras. A primeira e mais comum é aquela em que o leitor é quem lidera o processo de comunicação. A segunda acontece quando é a etiqueta que inicia a comunicação com o leitor. Esta última só acontece no caso de etiquetas activas. A electrónica residente na etiqueta possui duas funções principais: a primeira é recolher a energia electromagnética disponibilizada pelo campo electromagnético criado pelo leitor (no caso de etiquetas passivas); a segunda realiza a transmissão de um sinal modulado contendo a informação de identificação. Após a recepção do sinal, o leitor tem por missão descodifica-lo e enviar a informação obtida à aplicação informática que a tratará consoante as necessidades. O processo descrito pode ser observado na figura 4 [8]. Contudo, o funcionamento varia consoante a etiqueta possua o seu próprio sistema de alimentação (etiqueta activa) ou receba a alimentação do leitor (etiqueta passiva). O funcionamento da comunicação entre a etiqueta e o leitor, o acoplamento indutivo e as tecnologias de retro-espalhamento são temas abordados pormenorizadamente no próximo capítulo.

Tabela 1: Vantagens e desvantagens entre o código de barras e os sistemas RFID [7].

	Código de barras	RFID
Necessidade de estar à vista	Sim	Não
***Várias leituras* simultâneas**	Não	Sim
Diversificação	Baixa: podendo haver alterações no tamanho das etiquetas, feitas em papel ou plástico	Elevada: as etiquetas podem ter uma variedade de tamanhos, serem feitas a partir de diversos materiais
Resistência a líquidos, temperatura e químicos	Reduzida	Elevada
Modificação da informação que suporta	Não	Sim
Capacidade de armazenamento de dados	Até 50-bit para códigos de barra unidimensionais; até 3000 bit para os bidimensionais	Pode ir até aos *Mbytes*
Segurança (protecção dos dados)	Baixa	Elevada

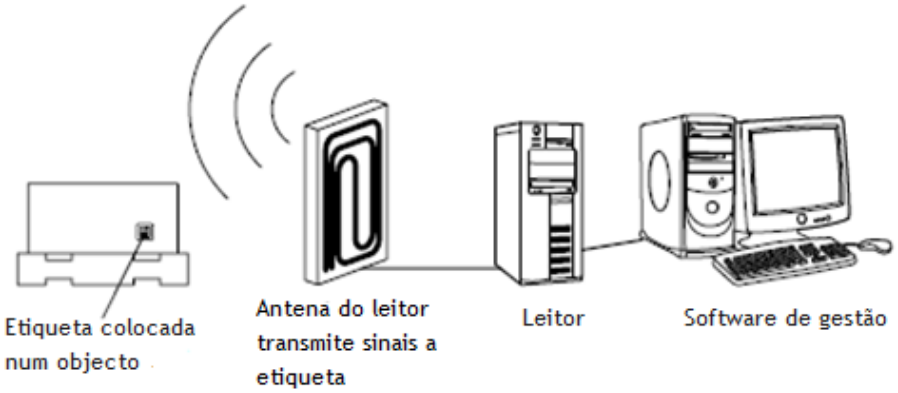


Figura 4: Esquema representativo do funcionamento de um sistema RFID **[8].**

2. Identificação por radiofrequência

Nos últimos anos, a identificação por radiofrequência tem vindo a ganhar cada vez mais popularidade, sendo que a primeira comercialização de um sistema RFID ocorreu na Noruega, em 1987, e era destinado à recolha de ferramentas. Assim, é cada vez mais possível encontrar aplicações que integram esta tecnologia, retirando benefícios da capacidade de identificação automática. Contudo, só na última década, é que se assistiu a um aumento significativo do interesse nesta tecnologia por parte das empresas, em parte promovido pela descida dos preços de produção [9]. O preço dos sistemas RFID depende de vários factores, tais como: a quantidade pretendida, o tipo de memória, ou o suporte do transdutor. De um modo geral as etiquetas activas são mais dispendiosas que as etiquetas passivas, sendo que estas podem custar entre 0,9€ e 0.85€ [10] e os leitores para este tipo de leitores custam aproximadamente 750€ [11].

2.1. Breve resenha histórica da tecnologia RFID

Desde que Guglielmo Marconi conseguiu transmitir sinais de rádio que atravessaram o Oceano Atlântico, em 1901, as ondas de rádio tornaram-se num importante suporte de comunicação. Este trabalho possibilitou o envio/recepção de informação em diferentes formatos, desde o código morse até à primeira chamada de voz.

Alexander Watson-Watt demonstrou em 1935 como localizar objectos físicos utilizando ondas de rádio. Não foi ele o "pai" do radar, pois foi um processo evolutivo, mas foi o primeiro a apresentar um sistema completo. Este aparelho emite ondas electromagnéticas que ao encontrarem um obstáculo são reflectidas de volta ao emissor. Uma análise do sinal reflectido permite determinar, para além da distância a que se encontra o objecto, se este se está a aproximar ou a afastar do emissor. Na Segunda Guerra Mundial, o radar foi um aparelho muito importante para os sistemas de defesa ingleses, já que permitia detectar a presença ou a ausência de aviões. Contudo, não permitia saber se estes eram aviões inimigos ou aliados. Os alemães, outros envolvidos nessa guerra, tinham o mesmo problema. Numa tentativa de solucionar a questão da identificação, manobravam os seus aviões em resposta ao sinal enviado pela estação em terra. Este processo provocava uma mudança na polarização de reflexão do radar, criando assim uma resposta distinta nos seus radares. Este sistema, apesar de rudimentar, foi a primeira aplicação da tecnologia de identificação utilizando ondas de radiofrequência. Em resposta, os ingleses criaram o IFF (*Identifier Friend or Foe*), que utilizava um *transponder* de longo alcance que modulava, de forma activa, o sinal de resposta ao sinal enviado pelo radar em terra. Isto permitiu tornar o processo de identificação dos aviões mais simples e rápido, deixando de ser necessário efectuar manobras como a anteriormente descrita [12].

Em paralelo, Harry Stockman da Força Aérea Americana publicou a primeira descrição pública da tecnologia RFID nomeada: "*Communications by Means of Reflected Power*". Nesse artigo, o autor descreve-nos a teoria básica da comunicação através da reflexão de energia, sendo abordadas a transmissão do radar (convencional), a comunicação por transmissão com alvos não reflectores e alguns métodos de modulação. Na conclusão do seu estudo, datado de 1948, Stockman refere-se à importante necessidade de desenvolver estudos e trabalhos futuros, com o intuito de explorar as diversas áreas de aplicabilidade da comunicação por reflexão de energia e ultrapassar algumas das barreiras por ele identificadas [13].

Depois dos estudos feitos por Stockman, foram necessários trinta anos e vários desenvolvimentos tecnológicos a nível da electrónica, tais como os desenvolvimentos do transístor, do circuito integrado, do microprocessador e dos sistemas de comunicações, para que a tecnologia RFID se tornasse efectivamente numa realidade. Os anos 60 e 70 foram palco de esforços comuns entre diversas identidades no estudo e desenvolvimento dos sistemas de RFID. Por exemplo, várias empresas, tais como a "Sensormatic", a "Checkpoint" e a "Knogo", juntaram-se e desenvolveram o EAS (*Electronic article Surveillance*). Este sistema utiliza uma etiqueta de um 1bit que nos indica unicamente a presença ou ausência da etiqueta. Estas etiquetas são feitas a um custo muito reduzido e permitem prevenir, de forma eficaz, o roubo de artigos. O EAS foi a primeira utilização comercial da tecnologia RFID e é, até à data, a mais difundida. Enquanto isso, na Universidade de Los Alamos foi desenvolvida e implementada uma etiqueta passiva que possui um alcance de funcionamento de uma dezena de metros [14].

Nos anos 80, as etiquetas foram submetidas a outros melhoramentos tais como a redução das suas dimensões físicas e aumento das suas funcionalidades, contribuindo para isso a utilização de circuitos integrados (CMOS) de baixo consumo energético. Em relação à memória, a EEPROM (*Electrically-Erasable Programmable Read-Only Memory*) torna-se na memória de eleição permitindo uma fabricação em grande escala.

Com a implementação e o disseminar da tecnologia RFID, tornava-se necessário uma normalização nessa área. Assim, uma organização que trabalha na área da criação e implementação de normas, a *Electronic Product Code Global*, criou o EPC (*Electronic Product Code*): um número de identificação universal, que atribui uma identidade única a um objecto. A Organização Internacional para a Padronização ("*International Organization for Standardization*" (ISO) foi outra organização que deu um importante contributo nesta área, criando e implementando normas para a identificação por radiofrequência [15]. No anexo A, encontram-se uma listagem das diversas normas.

Hoje em dia, a pesquisa e o desenvolvimento envolvendo os sistemas RFID continua bastante activa nas mais diversas áreas. Nos trabalhos publicados em [16] e [17], os autores têm como objectivo utilizar as etiquetas de RFID como sensores. Sendo que o primeiro

pretende criar uma etiqueta com tecnologia piezoeléctrica que recolhe energia (proveniente de vibrações) para se alimentar. Noutro trabalho [18] os autores apresentam um estudo sobre a modulação electromagnética, propagação das ondas EM e desenho de antenas com o intuito de criar uma etiqueta de RFID para utilização em aplicações médicas [19].

2.2. Aplicações da tecnologia RFID

Com o progresso da tecnologia, o potencial da identificação por radiofrequência aumentou, ao mesmo tempo que os custos de implementação foram decrescendo, cativando, assim, cada vez mais áreas de aplicabilidade [12, 20].

Uma análise da literatura permite agrupar as aplicações dos sistemas RFID às seguintes áreas de utilização: detecção de animais, aviação, controlo de acessos informático, gestão de edifícios, construção, tecido e roupas, controlo de acessos informáticos e dados nas empresas, retalho, segurança alimentar, livrarias, logística e gestão da cadeia de fornecimento, indústria mineira, construção e manutenção, museus, indústria automóvel e aeronáutica e saúde [20, 21].

Assim, a tecnologia de RFID é utilizada nas mais diversas áreas. A mais difundida tem a ver com o retalho, sendo que pode ser empregue com várias finalidades, desde a prevenção do roubo, passando pelo rastreio da mercadoria durante a expedição, até ao inventário automático de stock [22].

O rastreio de animais é outro domínio em que os sistemas RFID permitiram uma revolução na identificação, rastreio e estudo de animais. Na indústria agro-pecuária, a transacção e venda de animais está sujeita a leis que são cada vez mais rígidas, obrigando a uma identificação cada vez mais rigorosa do animal com informação tais como: a sua origem; o local de abate; o sexo do animal; e o seu número de identificação. Os sistemas RFID permitem de modo fácil e ágil registar todas essas informações, possibilitando o seguimento do animal em qualquer momento [23]. Na zoologia, incluindo a entomologia, os sistemas RFID permitiram abrir portas a novos estudos, senso que a identificação de insectos é usualmente realizada através da observação e anotações de características físicas, o que, por vezes, apresenta dificuldades. Aplicando uma etiqueta RFID nos insectos permite-nos recolher dados de forma automática, durante o período de tempo desejado, identificando cada insecto de forma fiável e fácil [24].

As livrarias e as bibliotecas são outra das áreas em que os sistemas RFID vieram facilitar a gestão do negócio. A primeira delas é, obviamente, a tarefa de inventariar, sendo que cada livro possui uma etiqueta de RFID com o seu próprio número de identificação. O inventário é realizado de forma rápida e automática, além de que os leitores de RFID podem

ler várias etiquetas em simultâneo, sem necessidade de manusear individualmente cada um dos livros. A segurança é outra funcionalidade que os sistemas RFID vieram reforçar. A maneira mais fácil é a de cada etiqueta possuir um bit de segurança. Este pode assumir o estado de entrada ou saída consoante se o utente requisitou o livro ou se o veio devolver. Se por acaso, o bit se encontra em modo de entrada, ao passar pelas portas de segurança um alarme será accionado [25]. Esta tecnologia pode também ser utilizada para a realização de estudos estatísticas, sendo que todos os dados são guardados pelo software, permitindo a sua utilização e consultadas para fins estatísticos.

Para além das vantagens já mencionadas, os sistemas RFID permitem acumular várias finalidades, poupando tempo e recursos. No capítulo quatro desta dissertação será estudada a aplicabilidade da tecnologia de RFID em meio hospitalar.

2.3. Princípios físicos da identificação por radiofrequência

A comunicação entre o leitor e a etiqueta de RFID pode ser realizada através de acoplamento indutivo ou através de retro-espalhamento (como veremos no ponto 2.3.3). Assim, é importante compreender os princípios físicos nos quais a tecnologia se baseia.

2.3.1. Campo magnético

Um campo magnético é criado pela movimentação de cargas eléctricas no vácuo ou num fio condutor, tal como podemos observar na figura 5.

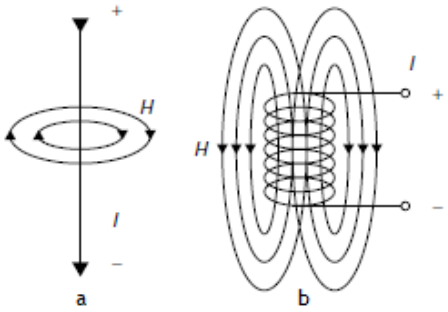


Figura 5: Campo magnético associado ao movimento de electrões: a) em torno de um fio; b) em torno de uma bobina. Sendo que H é a força do campo magnético e I a intensidade da corrente eléctrica [2].

No caso dos sistemas RFID, as ondas magnéticas são importantes, pois, para sistemas que comunicam via acoplamento indutivo, já que funcionam como suporte da comunicação. Neste tipo de sistemas é usual empregar antenas numa configuração em solenóide. Na figura 6, podemos observar as linhas de fluxo magnético em torno de uma bobina.

Como podemos observar na figura 6, quando um solenóide é percorrido por uma corrente eléctrica constante produz um campo magnético uniforme no seu interior, com linhas de indução paralelas ao eixo do solenóide, excepto nas proximidades das bordas. Contudo, se o fluxo magnético sofrer alterações, segundo a lei de Faraday, uma alteração do fluxo magnético irá induzir uma corrente [6].

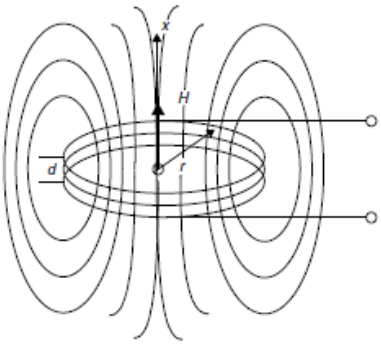


Figura 6: Comportamento das linhas de fluxo das ondas magnéticas em torno de uma bobina [2].

2.3.2. Ondas electromagnéticas

As ondas electromagnéticas, como o nome indica, são uma associação entre ondas eléctricas e ondas magnéticas, que conseguem viajar acopladas como podemos observar na figura 7.

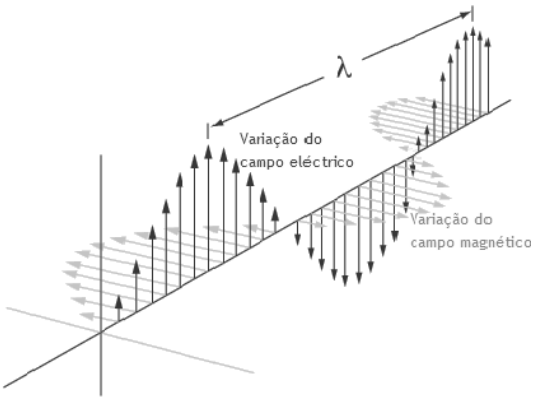


Figura 7: Onda electromagnética composta pelo campo magnético e pelo campo eléctrico. Os campos estão em fase, perpendiculares à direcção de propagação da onda.

As ondas electromagnéticas transportam energia armazenada nos campos magnéticos e eléctricos. Estes campos estão interligados perpendicularmente e variam ao mesmo tempo. No caso dos sistemas RFID, as ondas electromagnéticas são muito importantes, pois, vão definir o limite entre o campo próximo e distante e assim determinar a forma como a comunicação será efectuada: se por acoplamento indutivo ou por retro-espalhamento,

respectivamente [26]. Na tabela 2, abaixo, podemos encontrar um resumo das principais características do campo próximo e do campo distante.

Tabela 2: Principais características do campo próximo e do campo distante [27].

	Campo próximo	**Campo distante**
Definição	Região entre a antena do leitor e um comprimento de onda do campo magnético emitido pela antena do leitor	Região além de um comprimento de onda do campo electromagnético emitido pela antena do leitor
Intervalo do campo	A faixa de indução magnética é calculada pela seguinte fórmula: $c/2\pi f$, onde c é a velocidade da luz e f é a frequência de funcionamento. Assim, à medida que a frequência aumenta, a intensidade do campo magnético diminui	A faixa do campo distante é restringida à quantidade de energia recebida pela etiqueta e à sensibilidade do leitor ao sinal enviado pela etiqueta. As ondas electromagnéticas são atenuadas por 2 vezes: quando viajam do leitor para a etiqueta e da etiqueta para o leitor
Comunicação da etiqueta para o leitor	Modulação da amplitude do campo magnético	Modulação da amplitude do sinal reflectido ou retro-espalhado
Frequências	Baixas e altas	UHF e micro-ondas
Tipo de antena	Bobina ou solenóide	Dipolo
Zona de leitura	Reduzida	Maior
Complexidade	Baixa	Alta
Taxa de transferência de dados	Baixa	Alta

2.3.3. Comunicação entre as etiquetas e o leitor

A comunicação entre as etiquetas e o leitor, isto é, a troca de informação entre os dois componentes pode ser realizada, essencialmente, de duas maneiras diferentes: por acoplamento indutivo ou por retro-espalhamento [26].

No acoplamento indutivo, a energia é transferida de um circuito para o outro. Neste caso, como podemos observar na figura 8, o leitor de RFID vai gerar um campo magnético variável no tempo, o qual vai induzir uma corrente AC na etiqueta. De seguida, ocorre um processo de rectificação para que a electrónica da etiqueta possa utilizar a energia recebida.

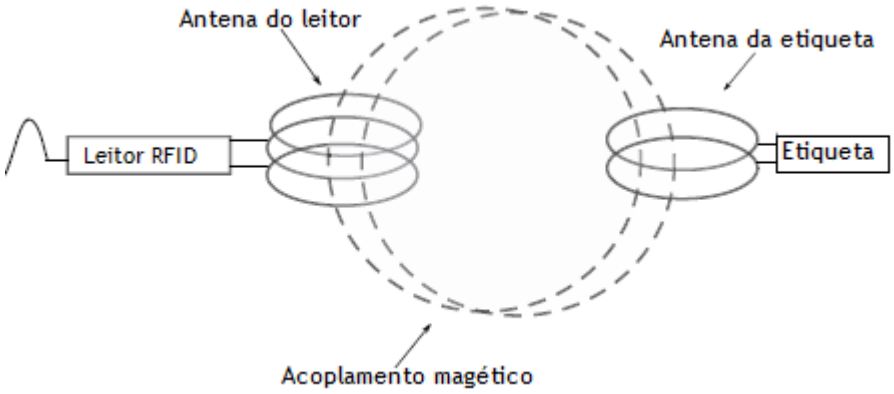


Figura 8: Comunicação entre o leitor e a etiqueta por acoplamento indutivo (campo próximo) [27].

Para reenviar a informação que contém, a etiqueta vai modular o sinal a transmitir. Este meio de comunicação pode ser empregue tanto em sistemas utilizando baixas frequências como em sistemas de altas frequências Para reenviar a informação que contém, a etiqueta vai modular o sinal a transmitir. Este meio de comunicação pode ser empregue tanto em sistemas utilizando baixas frequências como em sistemas de altas frequências, contudo, só funciona em sistemas de campo próximo de radiofrequência, pois, o leitor e a etiqueta têm que se encontrar a uma distância suficiente próxima para poderem partilhar um mesmo campo magnético [27, 26].

Assim, para os sistemas RFID que necessitam de um alcance mais longo, a transferência de energia é realizada através de ondas electromagnéticas, mais propriamente, através de retro espalhamento. Neste caso, o leitor produz uma onda electromagnética, variável no tempo, que induz uma corrente DC na etiqueta. Como resultado é gerada uma diferença de potencial na antena da etiqueta que vai permitir armazenar energia no *microchip*. A comunicação da etiqueta para o leitor é realizada através da variação da amplitude das ondas electromagnéticas (para modular o sinal) e enviar o sinal de volta ao leitor [27, 28]. Na figura 9, podemos observar um esquema representativo da comunicação via retro-espalhamento entre um leitor e etiqueta.

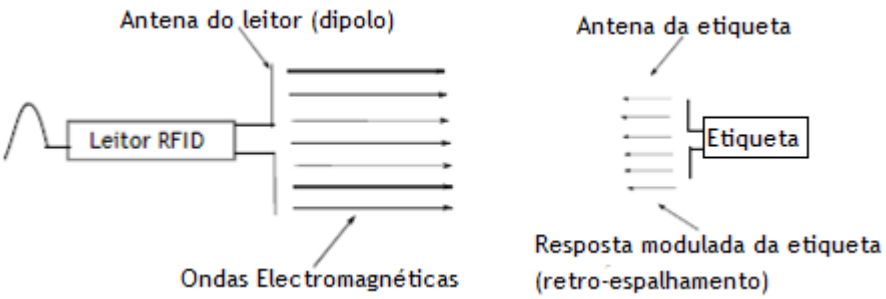


Figura 9: Comunicação entre leitor e etiqueta por retro-espalhamento (Campo longo) [27].

2.3.4. Frequências de funcionamento e normalização

Como o nome indica, a identificação por radiofrequência opera na gama das ondas de rádio, que vão desde os 3 KHz até aos 300 GHz. A gama de frequências pode dividir-se em baixas-frequências (*Low-frequency* - LF), altas-frequências (*High-frequency* - HF), ultra-altas-frequências (*Ultra High-frequency* - UHF) e as micro-ondas. Apesar destas frequências estarem todas englobadas na mesma gama do espectro electromagnético, têm características que as diferem. Assim, na tabela 3, encontram-se representadas as diferentes gamas das ondas de rádio e algumas das suas características mais importantes.

Com a difusão das tecnologias RFID, tornou-se necessária a normalização da identificação por radiofrequência. Assim, foram criadas normas para regular quatro áreas: a interface com o ar para frequências globalmente aceites, isto é, a forma como o leitor e a etiqueta comunicam; o teor e codificação dos dados, isto é, a forma como os dados são organizados ou formatados; a conformidade, isto é, os procedimentos específicos que nos permitem verificar se os equipamentos RFID e o seu desempenho estão em concordância com as normas; e por fim, a interoperabilidade entre o sistema RFID e as suas aplicações [29, 30].

A Organização Internacional para a Estandardização (ISO) e a *Electronic Product Code global* (EPCglobal) representam as duas principais organizações responsáveis pela criação das normas que gerem a tecnologia RFID. Contudo, esta última é a única a possuir um sistema que faz com que um determinado objecto possua a sua própria identificação, ou seja, um número único de identificação universal (EPC) [31].

Tabela 3: Frequências operacionais de radiofrequências e suas características para sistemas RFID [21, 29, 32].

Banda	LF	HF	UHF	Micro-ondas
Frequência	30-300 kHz	3 MHz- 30 MHz (13,56 MHz a mais usual)	300 MHz- 3GHz (433 MHz ou 865-956 MHz as mais usuais)	2-30GHz (2,45 GHZ a mais usual)
Alcance de leitura	<1 m	>1,5m	433 MHz é > 100 m 865- 956 MHz vai de 0,5 a 5 m	>10m
Memória	De 64 a 1360 bits	256 bits (8 blocos x 32 bits)	1 kbit	<1 kbit
Taxa de transferência de dados	<1 Kbit/s	Aproximadamente 25 kbit/s	De 30 a 100 Kbit/s	>100kbit/s
Características	Penetra a água mas não o metal	Penetra a água mas não o metal	Não penetra nem água nem metal	Não penetra água nem metal
Utilizações típicas	ID de animais Viação	Acessos, segurança,	Rastreamento, logística	Portagens

Na tabela 4, podemos encontrar referências às normas mais utilizadas consoante a frequência de utilização. Sendo que no anexo A se encontram as normas descriminadas.

Tabela 4: Normas mais utilizadas associadas as frequências globalmente aceites [33].

	LF	HF		UHF	UHF
	125/134,2 kHz	13,56 MHz	433 MHz	860-960 MHz	2,45 GHz
ISO	ISO 11784 ISO/IEC 18000-2ª ISO/IEC 18000-2B	ISO/IEC 14443 ISO/IEC 15693 ISO 18000-3	ISO 18000-7	ISO 18000-6A ISO 18000-6B ISO 18000-6C	ISO 18000-4 ISO/IEC 24730-2
EPC				Class 0 Class 1 Class 1 Gen 2	

2.4. Funcionamento dos sistemas RFID

2.4.1. Elementos

Num sistema RFID são necessários quatro componentes fundamentais para que este desempenhe a sua tarefa: um *transponder*, um *transceiver*, antenas (do leitor e outra da etiqueta) e o software de gestão. De seguida abordaremos cada um deles.

2.4.1.1. *Transponder* (ou etiqueta)

As etiquetas constituem o elemento que contem os dados e transportam na maior parte das vezes a identificação do objecto. Existem diversos tipos de etiquetas, tal como se representa na figura 10, mas, de um modo geral, podemos dizer que as etiquetas são constituídas por quatro componentes: uma antena, uma secção de radiofrequência (RF), uma secção digital e de rectificação (esta última unicamente para as etiquetas do tipo passivas) e, por fim, a unidade de memória [34]. É contudo importante salientar que a secção digital compreende ambas as subsecções analógica e digital. A antena vai receber o sinal e a secção de RF vai descodificar o sinal que vai de seguida ser convertido para o formato digital por um conversor analógico-digital. De seguida, o sinal é tratado pelo microcontrolador, que vai gerar um sinal de resposta. O sinal de resposta vai ser em seguida enviado para encriptação. O resultado é convertido num sinal analógico por um conversor digital-analógico (DAC). Por fim, o sinal é modulado e enviado ao leitor [34, 35].

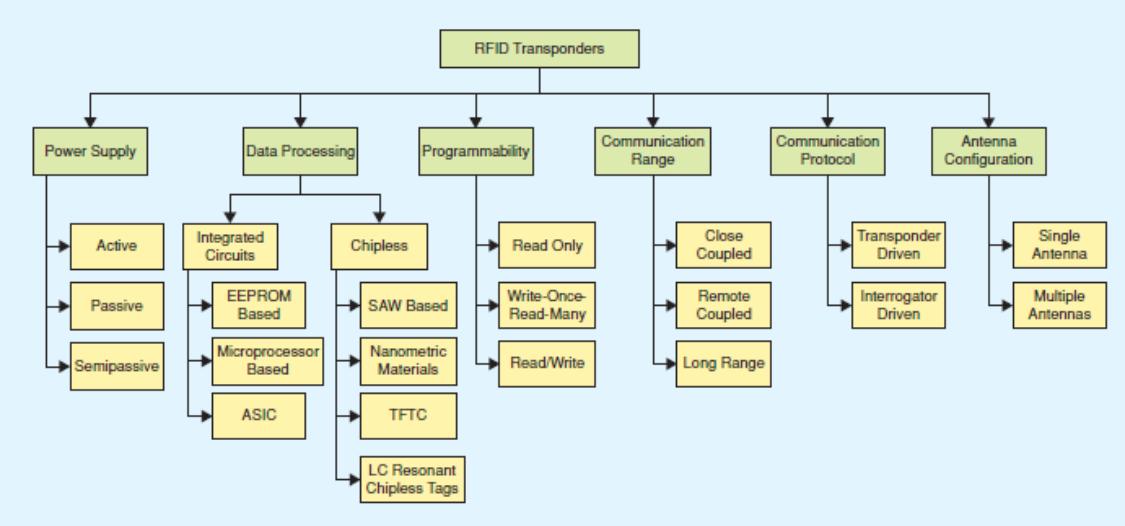


Figura 10: Classificações das etiquetas de RFID, retirado do artigo [35].

Como podemos observar na figura 10, existem diversas formas de classificar as etiquetas de RFID. Contudo, a mais popular e comummente difundida está relacionada com a forma de obtenção de energia. Assim, as etiquetas podem ser divididas em duas grandes categorias: activas e passivas, consoante a sua fonte de energia. As etiquetas activas possuem a sua própria fonte de energia, geralmente uma bateria; sendo que as etiquetas passivas obtêm a sua energia a partir do sinal de um leitor externo [9]. De um modo geral, as etiquetas são programadas com a informação que as identifica, apesar das etiquetas activas poderem conter mais informações, passíveis de serem alteradas [8].

Etiquetas activas:

Como foi referido acima, as etiquetas activas possuem a sua própria fonte de energia. Este factor confere-lhes um sinal mais forte e, por conseguinte, os seus leitores possuem um maior raio de alcance. Contudo, o facto de possuírem uma bateria faz com que tenham maiores dimensões, sejam mais dispendiosas, o que determina que estas operem em frequências mais elevadas: geralmente 455 MHz, 2,45 GHz (dependendo do alcance de leitura da aplicação e da memoria exigida) [9]. Porém, este acréscimo de tamanho comparativamente às etiquetas passivas proporciona-lhes uma maior capacidade de memória, o que lhes permite conter não só o número de identificação, mas também informações relevantes, tais como: a origem e o destino de um produto, a informação sobre um paciente, entre outras. É importante salientar que este tipo de etiquetas pode permanecer inactiva, poupando assim bateria e aumentando a sua longevidade, até entrarem no raio de alcance do leitor ou podem transmitir um sinal, a um intervalo de tempo pré-programado. Apesar de

serem mais dispendiosas, as etiquetas activas têm provado o seu valor, sendo que em muitas aplicações se observa um rápido retorno económico do investimento realizado [8].

É também importante salientar que, nas etiquetas activas, a secção digital fornece a número de identificação (ID) e incorpora os protocolos de segurança e de encriptação, sendo que o processador controla o processamento de dados e os protocolos de comunicação [35].

Etiquetas passivas:

Como já foi acima referido, as etiquetas passivas não possuem nenhuma bateria ou qualquer outra fonte própria de energia. Estas obtêm-na do campo electromagnético produzido pelo leitor, quando penetram no raio de alcance deste. Assim, para recolher essa energia, todas as etiquetas do tipo passivas possuem um *front end* de RF (composto pela antena e pelo circuito de adaptação de carga) e um circuito analógico (composto por um circuito LC e um rectificador). As etiquetas mais complexas podem possuir ainda um circuito digital que pode ser do tipo IC, ASIC ou um bloco de memória. O *front- end* de RF tem como finalidade minimizar a reflexão do sinal e maximizar a energia transferida entre a antena e o circuito da etiqueta. A função do rectificador é a de converter a tensão AC em DC [35]. Na figura 11, podemos encontrar um esquema detalhado de um rectificador de tensão de uma etiqueta passiva. Nesse esquema podemos observar que na saída do rectificador se encontra um *buffer*, que vai armazenar a energia rectificada, garantindo assim energia suficiente para proceder às operações de modulação e retro-espalhamento do sinal [36].

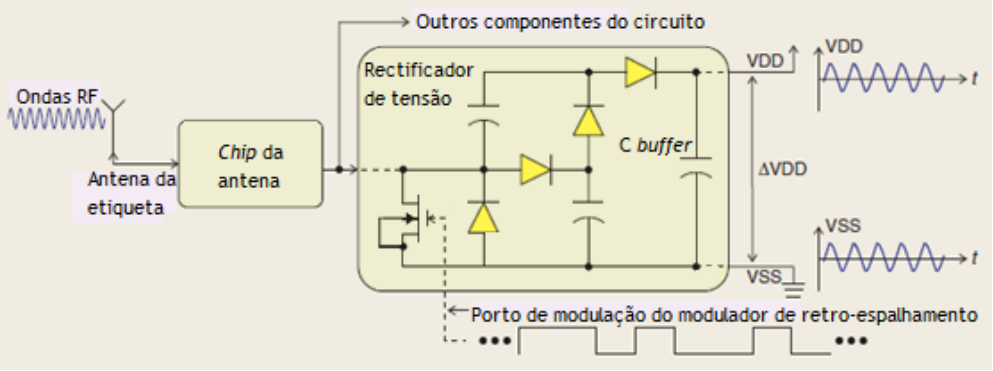


Figura 11: Esquema detalhado de um rectificador de tensão de uma etiqueta passiva [36].

Desta feita, podem apresentar menores dimensões e, em consequência disso, serem muito mais económicas. Este factor faz com que possam ser integradas em cada vez mais materiais, produtos e aplicações [8, 14].

Devido ao seu baixo custo, a etiqueta passiva fará parte, provavelmente, da maior parte das implementações de identificação por radiofrequência [9].

Na tabela abaixo, encontram-se algumas comparações pertinentes entre etiquetas activas e passivas:

Tabela 5: Etiquetas activas vs etiquetas passivas [8].

Etiquetas	Activas	Passivas
Tempo de vida	Igual ao tempo de vida da bateria	Virtualmente ilimitada
Tamanho	Na ordem de um a uma dezena de centímetros	Na ordem do micro até alguns centímetros
Alcance de leitura (varia com a frequência utilizada)	Desde 20 m e pode ultrapassar os 100 m	Vai desde alguns milímetros até aproximadamente 3 m
Potenciais interferências	São menos sensíveis, contudo podem ocorrer se a etiqueta se encontrar dentre de um contentor metálico	Sensíveis a alguns tipos de metais e líquidos

Porém, é importante salientar que existe uma terceira classe de etiquetas: as etiquetas semi-passivas. Estas possuem uma bateria que alimenta a electrónica da etiqueta, contudo, para comunicar recorrem à energia enviada pelo leitor [12].

De um modo geral, como já foi referido, as etiquetas são classificadas relativamente à sua fonte de energia. Contudo, estas também podem ser classificadas em relação à sua configuração. Teremos então 3 classes diferentes.

As etiquetas *Read Only* (RO), que são unicamente de leitura, são programadas no decorrer do processo de fabricação e os dados que contêm não podem ser alterados. As etiquetas *Write Once - Read Many* (WORM) são programadas uma vez, geralmente pelo utilizador, e não pelo fabricante. Na prática, as etiquetas WORM podem ser reprogramadas diversas vezes, porém, se o limite de reescrita for ultrapassado, a etiqueta pode ser permanentemente danificada. As etiquetas do tipo *Read/Write* (RW) podem ser programadas inúmeras vezes (aproximadamente 100.000 vezes). Este tipo de etiquetas possui geralmente uma memória do tipo Flash ou EEPROM [35].

2.4.1.2. Leitor RFID

O leitor, de um modo geral, serve para activar e controlar a comunicação com a etiqueta. É também dele a responsabilidade de gerir a transferência de dados entre as etiquetas e a aplicação de software. Desta feita, o leitor é inteiramente responsável por executar as comunicações, realizar os procedimentos de autenticação e de anti-colisão. Os leitores são constituídos fundamentalmente por dois blocos: o sistema de controlo e o bloco de interface de alta frequência (*HF Frequency*). Sendo que, como podemos observar na figura 12, o sistema de controlo é a componente do leitor que comunica com a aplicação de software e a interface de alta frequência com o *transponder*. Já de seguida são abordadas mais detalhadamente as funções de cada um dos elementos.

A unidade de controlo do leitor é responsável pelas funções de comunicação com a aplicação de software e execução dos seus comandos, controlo da comunicação com o *transponder* (*via "master-slave"*), codificação e descodificação de sinais, execução de um algoritmo anti-colisão, encriptação e desencriptação dos dados transferidos e autenticação da etiqueta pelo leitor [6, 35].

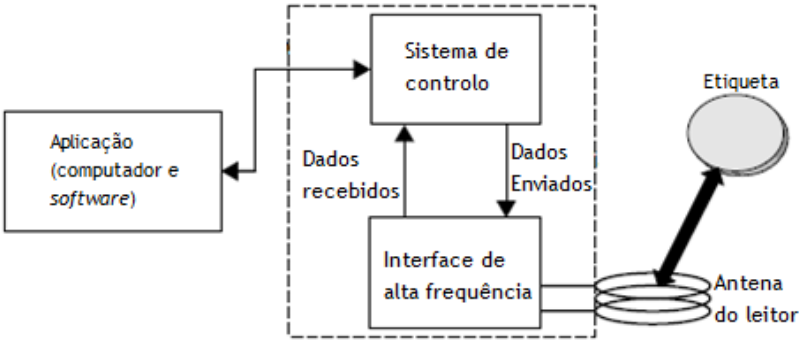


Figura 12: Esquema representativo da organização de um leitor [6].

No entanto, é importante salientar que as três últimas características se encontram unicamente em sistemas mais complexos, pois, para poder efectuar estas funções, os leitores têm que estar equipados com um módulo ASIC, um circuito integrado de aplicação específica, ou com um processador de sinais digitais (DSP), que vai converter ondas electromagnéticas em informação digital. Para implementar os protocolos de anti-colisão, alguns necessitam de várias antenas sendo que, apenas uma pode estar activa num dado instante, sendo nestes casos necessário incluir um multiplexador. Estas unidades de controlo apoiam-se em microprocessadores para efectuar todas estas funções. Contudo, com o intuito de não sobrecarregar o microprocessador, estas unidades de controlo estão também providas com um módulo ASIC, sendo que, para obter um melhor desempenho será acedido através do barramento do microprocessador. É também importante salientar que a troca de dados entre

a unidade de controlo do leitor e o software é efectuada através de uma interface standard do tipo RS-232 ou RS-485. Como podemos verificar na figura 13, o sistema de controlo do leitor de RFID é composto por um microprocessador (muita das vezes um DSP), um bloco de memória (RAM/ROM), um módulo ASIC e um bloco de comunicação, geralmente RS-232 ou RS-485 [6].

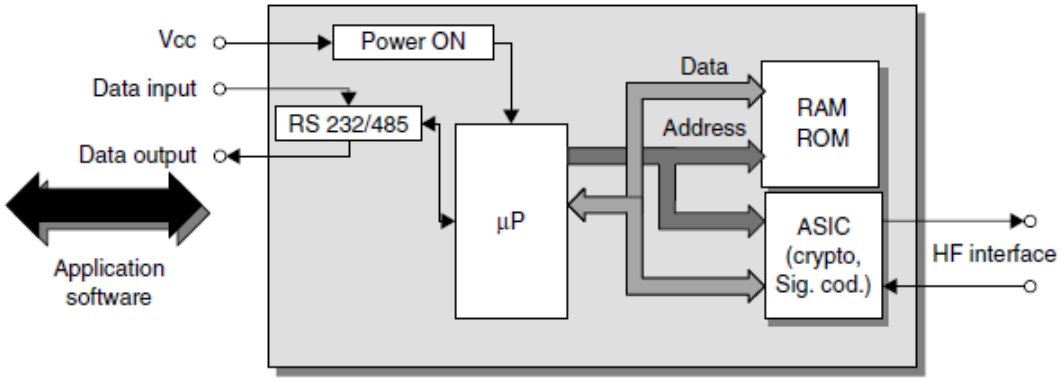


Figura 13: Esquema representativo da organização da unidade de controlo de um leitor [6].

A interface de alta frequência (*HF frequency*) é responsável pela produção de energia de transmissão de alta frequência para activar a etiqueta e fornecer-lhe a energia necessária; pela modulação do sinal de transmissão para envio dos dados para as etiquetas; e pela recepção e demodulação dos sinais enviados pelo *transponder*, usualmente, através de *Ampiltude Shift Keying* (ASK) ou *bi-phase Shift Keying* (BPSK) [6, 35].

Como podemos observar na figura 14, a interface de alta frequência, é formada por duas vias de sinais: a via de transmissão de dados e a via de recepção de dados. A primeira é composta por um oscilador, um modulador e por um módulo de saída. Em relação à segunda, a via de recepção de dados, é constituída por um filtro passa-banda, um amplificador e um *demodulador*. É importante salientar que os leitores de RFID podem ser classificados de diversos modos. Um deles relaciona-se com a forma como o leitor adquire a sua energia. Se a obtém da rede é um dispositivo fixo, se de uma bateria é geralmente um equipamento portátil. Em ambos os casos, são alimentados por uma tensão entre os 5 e os 12 Volts [35].

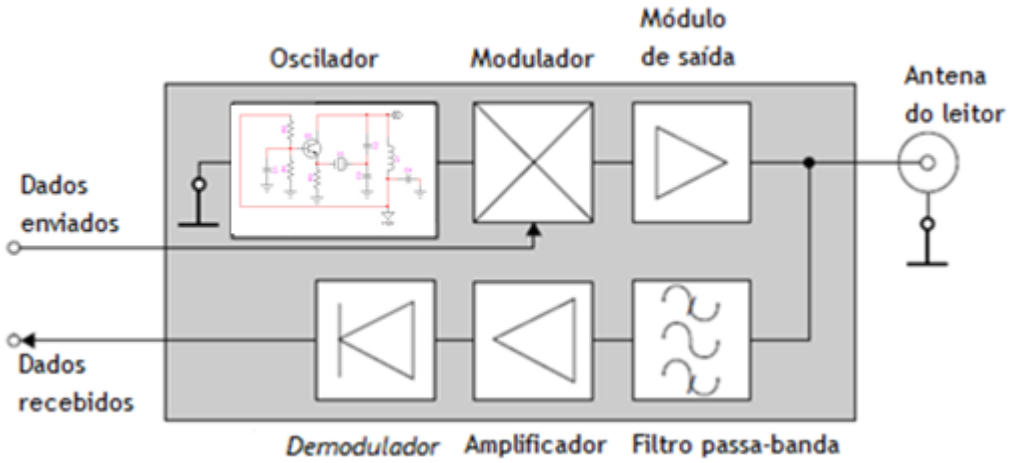


Figura 14: Esquema representativo de uma interface de alta frequência (para um sistema de acoplamento indutivo) [6].

2.4.1.3. Antena RFID

A antena é um dos elementos chave nos sistemas RFID pois, a performance da antena, seja do leitor ou da etiqueta, tem um efeito significativo na distância de alcance do leitor e na detecção apurada de um sistema RFID. Outra das formas de classificar os sistemas RFID é dividi-los em comunicação por campo de curta distância e comunicação por campo de longa distância. As antenas podem ser agrupadas em antenas de curtas distâncias e de longas distâncias, consoante o tipo de comunicação que permitem. As antenas de campo longo são utilizadas no caso em que é necessário cobrir longas distâncias ou frequências altas (UHF e micro-ondas) e são mais sensíveis ao ambiente envolvente como aos líquidos ou aos metais. As antenas de campo curto são utilizadas para distâncias curtas e frequências de utilização baixa, LF e HF [26].

As antenas de campo curto empregam geralmente antenas de *loop* devido aos leitores, da maioria de sistemas RFID, serem baseadas no acoplamento indutivo e no poder de transferência e de comunicação das etiquetas. Quando a frequência atinge a banda de UHF, as antenas convencionais (*solid-line loop)* não são aconselhadas, uma vez que o perímetro do *loop* da antena pode não ser suficiente para ter uma cobertura eficiente. Isto acontece porque a parte eléctrica do *loop* da antena não pode gerar uma boa distribuição do campo magnético na zona do campo próximo da mesma, pois, a distribuição da corrente ao longo do *loop* experimenta uma inversão de fase e uma corrente nula, pondo em causa a fiabilidade do sistema RFID. Em relação às antenas de campo longo, podem ser de diversos tipos. As mais comummente utilizadas são as antenas circulares polarizadas que detectam as etiquetas independentemente das suas orientações. Nas aplicações em que são empregues etiquetas com orientação fixa podem ser utilizadas antenas de dipolo [37].

No projecto e desenvolvimento de uma antena de campo longo eficiente e sustentável, neste caso para aplicação RFID, é importante ter em consideração alguns critérios, sendo os mais importantes: a frequência de alcance, a largura de banda, a polarização, o ganho, a impedância, o tamanho, o custo e a robustez mecânica. Sendo que as etiquetas são, basicamente, constituídas pela antena, um *microchip* e uma bateria (no caso de etiquetas activas). Para um funcionamento óptimo, a escolha da antena da etiqueta tem de ser baseada em requisitos importantes:

- Deve receber um sinal óptimo do leitor para carregar o *microchip*. No caso de antenas de campo longo têm que ser concordantes com o *microchip*. Em relação às antenas de campo curto (bobinas), é necessário que a indutância seja adequada à configuração do circuito ressonante;
- É necessário que seja de tamanho reduzido para poder ser colocada ou inserida nos objectos a serem rastreados;
- Insensibilidade ao objecto ou material ao qual for ligado para manter o funcionamento consistente;
- Necessários padrões de radiação (gráfico da distribuição relativa da radiação emitida pela antena no espaço);
- Estrutura robusta;
- Ser de baixo custo de produção [37].

2.4.1.4. Aplicações de Middleware

As aplicações de *middleware* têm como principal função gerir os leitores e os dados provenientes das etiquetas. Assim, recebe múltiplos sinais provenientes de uma etiqueta e converte-os num único sinal de identificação. É também ele que faz a ligação entre os vários elementos de hardware e as diversas aplicações de software de um sistema RFID [8].

A aplicação de *middleware* inclui as seguintes características:

- **Gestão de dispositivos:** a aplicação de *middleware* de um sistema RFID permite aos utilizadores configurar, monitorizar, implantar e executar comandos directamente para leitores agindo como uma interface comum;
- **Gestão de dados:** depois de captar os dados, a aplicação de *middleware* também permite filtra-los e envia-los para o endereço apropriado;
- **Integrações de aplicações:** a aplicação de *middleware* de um sistema RFID fornece as mensagens, encaminhamento e características de ligação necessárias à integração dos dados RFID, adquiridos na gestão de uma cadeia de fornecimento já existente, no planeamento de recursos da empresa, ou na gestão de armazéns;

- **Integração de parceiros:** a aplicação de *middleware* pode igualmente fornecer soluções de colaboração entre diversos parceiros comerciais, como por exemplo o "buisiness-to buisiness" (B2B) [8, 38].

Como podemos observar na figura 15, a aplicação de *middleware* pode ser composta por duas interfaces de comunicação: a interface de comunicação responsável pela interacção com as aplicações externas e a interface de leitores que lida com os leitores. Esta estrutura possibilita que as aplicações externas e os serviços cooperem com cada um dos leitores ligados à aplicação de *middleware* [38].

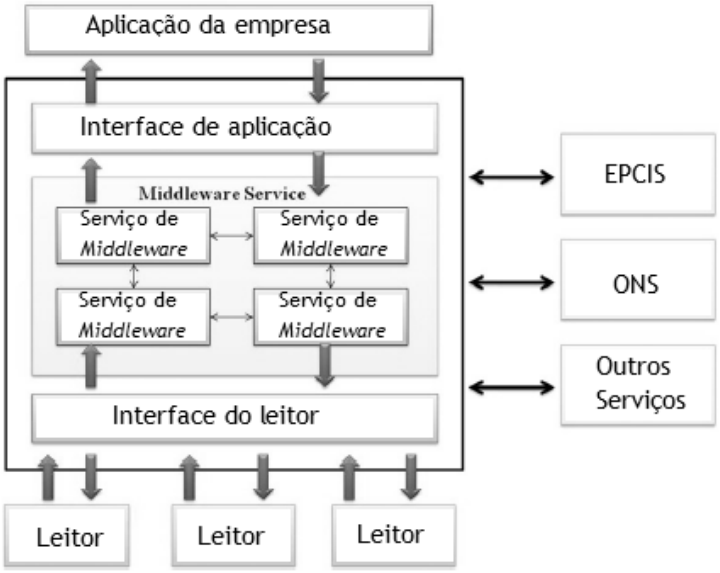


Figura 15: Esquema representativo da organização da aplicação de middleware [38].

No caso específico de uma utilização hospitalar, a aplicação de *middleware* permite um rápido acesso aos leitores, diminui o volume de informação que as aplicações médicas têm que processar, agrupando e filtrando as informações provenientes do leitor e enviando-as para as devidas aplicações médicas. Este monitoriza assim as componentes físicas do sistema [39].

2.5. Segurança em RFID

Como foi visto anteriormente, a identificação por radiofrequência é uma tecnologia que permite uma identificação de forma automática utilizando ondas de rádio para à transmissão de dados. Por ser *wireless*, é importante que estes sistemas possuam um bom sistema de segurança. Pois, se um sistema não for protegido qualquer leitor pode aceder à informação nele contido [40]. Nesse sentido, existem diversos trabalhos e estudos relativos à

segurança em sistemas de RFID. Nos artigos [41-43] podemos encontrar um levantamento dos possíveis problemas de privacidade e segurança em sistemas RFID. É dada especial ênfase ao rastreamento, isto é, à localização contínua de pessoas e de bens, ao acesso indevido às informações privadas ou pessoais contidas nas etiquetas, bem como às abordagens científicas já existentes na prevenção desses riscos. Apesar das ameaças abordadas serem as mesmas, no trabalho desenvolvido por Mohd F. Mubarak [44], a abordagem difere um pouco das restantes, sendo que, os autores agrupam e diferenciam ataques activos de ataques passivos. As ameaças do tipo passivo, como a espionagem (intercepção da ondas de radiofrequência), não interferem nas comunicações mas constituem um ataque à privacidade e ao anonimato das comunicações. Por sua vez, os ataques do tipo activo geram interrupções ou interferências nas comunicações entre o leitor e as etiquetas.

São abordadas de seguida os diferentes tipos de ameaças consideradas por alguns autores, assim como soluções para prevenir estes ataques.

2.5.1. Ameaças à segurança dos sistemas RFID

As ameaças aos sistemas RFID podem ter diversas origens, sendo que existem vários modos de classificação. Contudo, aquele que melhor agrupa e relaciona o maior número de ameaças à segurança de um sistema RFID - de acordo com a pesquisa realizada - será a classificação apresentada por Ding Zhen-hua, apresentada na tabela 6, na página seguinte [45].

As ameaças à camada física corrompem as propriedades do sinal de radiofrequência, tais como, a frequência e o portador do ciclo de relógio. Esta categoria engloba os ataques por intercepção das ondas de radiofrequência, interferências e a clonagem. A intercepção das ondas de radiofrequência (ou espionagem) ocorre quando um intruso intercepta dados com um leitor compatível com a família de etiquetas e frequência utilizada, aquando da comunicação entre a etiqueta e o seu leitor. É importante salientar que o leitor do intruso é previamente ligado a um osciloscópio digital, gravando assim o sinal captado pela antena. Para impedir a espionagem existem diversas abordagens tais como a utilização de um canal seguro ou a criptografia. As interferências podem ocorrer com a existência de ruído [46].

Quanto à clonagem, como as etiquetas são usualmente de baixo custo e tecnologia simples, estas são facilmente clonadas. A clonagem acontece quando leitores não pertencentes ao sistema RFID conseguem capturar a informação identificativa da etiqueta. Este ataque é perigoso na medida em que podem ajudar na contrafacção de, por exemplo, passaportes ou em meio hospitalar alteração das etiquetas dos medicamentos [47].

Tabela 6: Ameaças à segurança e privacidade em sistemas RFID [45].

Ameaças à segurança dos sistemas RFID	
Ameaças à camada física	Intercepção das ondas de RF
	Interferências
	Clonagem
Ameaças à camada de comunicação	Colisão
Ameaças à camada de aplicação	Falsificação
	Replay
	Rastreamento
	Dessincronização
	Vírus

As colisões são as principais ameaças à camada de comunicação. As colisões ocorrem quando várias etiquetas respondem ao mesmo tempo à solicitação de um leitor. Para impedir estas situações existem diversos protocolos para coordenar as respostas das etiquetas. Mas as colisões e os protocolos anti-colisões serão abordados mais detalhadamente no subcapítulo 2.6.

As ameaças à camada de aplicação violam principalmente as propriedades tais como, a identificação da etiqueta, a operação relacionada com o *back-end* da base de dados e a privacidade. Estas ameaças englobam a falsificação (das etiquetas), *replay*, rastreamento, dessincronização e vírus. As falsificações advêm do esquecimento de uma etiqueta, contudo, esta continua activa e é utilizada por outra pessoa ou entidade. As ameaças do tipo *replay* atacam todos os sistemas sendo que esgota os recursos computacionais do leitor, da etiqueta e do sistema de *back-end* da base de dados. Isto acontece porque neste tipo de ataque a etiqueta é solicitada inúmeras vezes. Em relação ao rastreamento, estas ameaças podem por em risco a privacidade dos portadores de etiquetas. As ameaças por dessincronização, como o próprio nome indica, vão levar a uma perda de sincronização do número de identificação entre o servidor da base de dados e a etiqueta. A última ameaça incluída nas ameaças de aplicação é o vírus. Os sistemas RFID infectados podem atacar o servidor da base de dados ou pior, derrubar todo o sistema [45].

2.5.2. Soluções para garantir a segurança de sistemas RFID

Para impulsionar a aceitação da tecnologia RFID foi necessário encontrar soluções para proteger os dados contidos na etiqueta. Assim, várias técnicas foram desenvolvidas. Um dos mais simples métodos consiste em "matar" a etiqueta. Neste procedimento, cada etiqueta possui um código único de 24 bits, que foi programado aquando da sua criação. Quando este código lhe é enviado, esta desactiva-se para sempre. Outro método similar consiste em adormecer a etiqueta. O sistema é o mesmo, contudo, a etiqueta pode ser reactivada com o código. Estes dois processos não são totalmente fiáveis, pois, devido à sua utilização, certas etiquetas não podem ser desactivas definitivamente ou temporariamente. Sendo que neste último caso, o facto de as adormecer não impede que uma pessoa indesejada possa aceder à informação nelas contidas [41].

Outro método consiste em utilizar um bloqueador de etiqueta. Este bloqueador consiste numa etiqueta que previne varrimentos indesejados de etiquetas contidas em zonas ditas como privadas. Estas etiquetas possuem um bit de privacidade. Quando este está a "0": a etiqueta está marcada como privada. Nestes casos, os bloqueadores de etiquetas mais simples, meramente enviam uma mensagem ao leitor do tipo: "não ler etiqueta privada". No caso de bloqueadores de etiquetas mais efectivos, estes impendem o varrimento indesejado utilizando um protocolo de anti-colisão chamado "*singulation*". Este protocolo faz com que os sinais das diversas etiquetas não interfiram uns com os outros [42].

Este protocolo será abordado mais profundamente no subcapítulo relativo à anti--colisão.

A protecção de dados é alcançada nos computadores e na internet através da utilização de vários métodos. A criptografia é uma das melhores opções na protecção de informação em canais de comunicação [44]. Numa comunicação criptograficamente segura, os dados (ou mensagem), juntamente com uma chave criptográfica, são a entrada para o algoritmo criptográfico. A saída será o texto cifrado [48].

Em sistemas RFID podem ser empregues diversos métodos de criptografia que se podem dividir em dois grupos principais: criptografia simétrica (ou criptografia de chave privada) e criptografia assimétrica (ou criptografia de chave publica) [49].

Na criptografia simétrica, é aplicada uma chave aos dados para serem cifrados, sendo esta chave dita privada, pois, só a etiqueta e os leitores do sistema a devem possuir [50]. Assim, um leitor só poderá decifrar os dados contidos na etiqueta se possuir a chave. Na tecnologia de identificação por radiofrequência o mais usado é o AES ("Advanced Encryption Standard") [42].

O AES é uma cifra que processa blocos de dados de 128-bit. Este é um algoritmo que opera em blocos de dados denominados de "Estado". Cada Estado constitui uma matriz de

quatro colunas e quatro linhas de bits. O metodo pode utilizar chaves de 128, 192 ou 256 bits que convertem o texto original em texto cifrado através de 10, 12 ou 14 iterações, respectivamente. Cada iteração é composta por 4 etapas de processamento:

- "*SubBytes*": é uma etapa de substituição não linear onde cada byte é substituído por outro, utilizando uma S-Box;
- "*ShiftRows*": cada linha de Estado avança de um determinado número de posições para a esquerda, ciclicamente;
- "*MixColumns*": cada coluna é multiplicada por um polinomial fixo: $2^{8,}$ denominado de corpo de Galois;
- "*AddRoundKey*": é aplicada um XOR, bit a bit, entre o Estado e uma sub--chave própria de cada turno. Esta é derivada da chave principal [51].

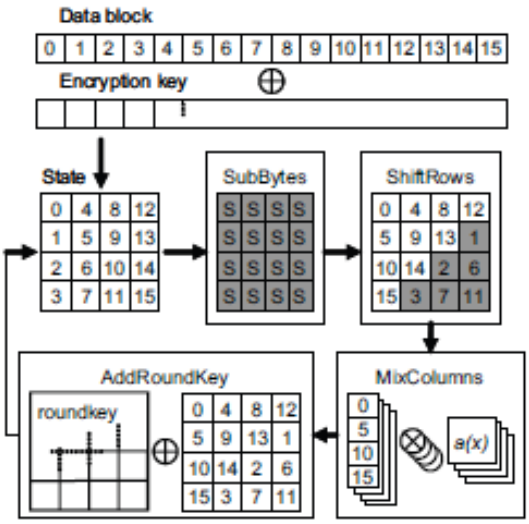


Figura 16: Esquema representativo das diversas etapas de cada iteração do AES (SubBytes, ShiftRows, MixColumns e AddRoundKey) [51].

No trabalho [52] podemos encontrar uma implementação, bem-sucedida, do algoritmo AES numa etiqueta do tipo passiva numa frequência de 13,56 MHz. Como podemos observar na figura 17a), a etiqueta com segurança reforçada é constituída por 4 partes: a interface analógica (gera e distribui a energia recebida do leitor, modulação e demodulação do sinal e recuperação do relógio), a unidade de controlo digital (trata da comunicação com o leitor, implementa os mecanismos de anti-colisão, executa os protocolos e permite o acesso para leitura e escrita na EEPROM e modulo AES). Por seu lado a EEPROM armazena dados específicos da etiqueta e as chaves criptográficas, enquanto que o módulo AES é responsável pela criptografia e autentificação das etiquetas. Em detalhe, o módulo AES, é composto por 3 componentes. Em primeiro, podemos encontrar um controlador que é responsável pela comunicação com os outros módulos da etiqueta (para troca de dados), sequência as 10

iterações da criptografia AES, além do que, endereça a RAM e gera sinais de controlo para o *datapath*. A RAM armazena o "Estado" (de 128 bits) e a chave de também 128 bits. Por fim, o *datapath* vai calcular as transformações das etapas *SubBytes*, *Mixcolumns* e *AddRoundKey*. A etapa *SubBytes* é implementada pelo controlador. Na figura 17b) podemos observar um esquema representativo do módulo AES.

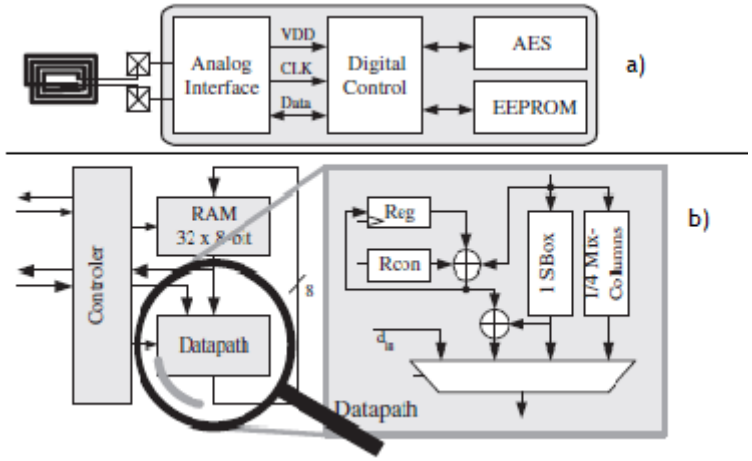


Figura 17: a) Esquema de uma etiqueta com segurança reforçada com um módulo AES; b) Esquema das componentes do módulo AES e do datapath do mesmo [52].

Para se adequar o protocolo de encriptação AES à tecnologia RFID, tem que se garantir uma implementação de baixo custo, um desempenho energético bom, e um tamanho reduzido. Assim, para diminuir o consumo energético deste módulo, o relógio interno passou dos 13,56 MHz iniciais para os 100 KHz. Porém, não foi a única modificação efectuada. Como referido acima, a tecnologia AES é implementada com 128-bit, mas para este protocolo foi implementado uma arquitectura AES de 8-bit por duas razões. A primeira proporciona uma poupança nos recursos de silício (área de implementação), pois esta arquitectura só necessita uma S-Box. Em segundo lugar, as operações de 8-bit consomem significativamente menos energia. Assim, é importante salientar que a diminuição do número de S-Boxs vai provocar um aumento de ciclos de relógio aquando da criptografia, sendo esta uma pequena desvantagem. Para resumir, os autores deste trabalho conseguiram implementar um protocolo AES de baixo consumo energético e de pequenas dimensões. Este módulo é possuidor de um chip com 3 595 portas lógicas, que requerem 8,15 µA, quando opera a uma frequência de 100 kHz [52].

Ao contrário da criptografia simétrica, a criptografia assimétrica utiliza duas chaves. Cada entidade possui portanto um par de chaves: uma publica que é disponibilizada para quem pretende enviar uma mensagem cifrada e uma privada mantida secreta. Qualquer entidade pode enviar uma mensagem confidencial usando apenas a chave pública. No entanto, esta só pode ser decifrada com uma chave privada, que esta na posse do destinatário. É importante salientar que neste tipo de criptografia, a chave privada e a chave

pública são relacionadas matematicamente. Para além de ser utilizada para protecção da privacidade, a criptografia de chave pública também pode ser utilizada para autentificação (assinaturas digitais). Como exemplo de criptografia assimétrica temos a recriptografia e a recriptografia universal. Como os nomes indicam, estes métodos cifram por diversas vezes os dados, utilizando o processo descrito acima. Estas duas técnicas apresentam algumas diferenças. Ao contrário da recriptografia, onde é utilizada apenas um par de chaves, na recriptografia universal o número de pares aumenta. Além de não haver necessidade de se conhecer a chave pública associada para poder reencriptar os dados [50].

É importante salientar que tanto a criptografia simétrica como a assimétrica possuem vantagens e desvantagens. Na tabela 7 é realizada uma comparação entre elas.

Tabela 7: Tabela comparativa entre a criptografia simétrica e a criptografia de chave pública [50, 52].

	Criptografia Simétrica	**Criptografia Assimétrica**
Gestão e transmissão de chave	Necessita de uma rede bem segura, pois a chave que permite a codificação é a mesma que descodifica	Não necessita de rede segura mas um directório seguro onde guardar as chaves públicas associadas a cada entidade
Recursos computacionais e energéticos necessários	Relativamente baixos	Elevados
Custo e dificuldade de implementação	Baixos	Elevados
Desencriptação	Necessita de várias desencriptações (iterações) ou o leitor tem que estar sincronizado com a etiqueta	A desencriptação é efectuada logo à primeira
Tempo de desencriptação	Rápido	Lento

Devido à necessidade de serem de baixo custo, é importante ter em consideração que a grande maioria das etiquetas não possui recursos adequados para criptografia. Tipicamente, estas podem armazenar umas centenas de bits e possuem aproximadamente entre 5000 a 10000 portas lógicas, sendo que 250 a 30000 delas podem ser reservadas para funções de segurança [43]. Assim, para uma melhor aproveitamento é preferível proceder à criptografia dos dados no leitor e enviar a mensagem já cifrada para as etiquetas [44].

2.6. Protocolos anti-colisão

O facto de na tecnologia RFID o leitor ser capaz de ler diversas etiquetas simultaneamente é uma grande vantagem em relação a outras tecnologias de identificação. Quando várias etiquetas respondem ao mesmo tempo à solicitação de um mesmo leitor, o sinal de umas pode interferir com o sinal de outras, provocando assim uma colisão de dados. Para além de causar problemas na leitura das etiquetas, as colisões induzem também a um desperdício de largura de banda, de energia, e a um aumento do tempo de identificação [10, 27, 53].

Assim, percebemos que os protocolos anti-colisão são cruciais para o óptimo funcionamento de sistemas de RFID com várias etiquetas. Estes podem ser agrupados em diversas categorias: SDMA (Acesso Múltiplo por divisão de Espaço), FDMA (Acesso Múltiplo por Divisão de Frequências), CDMA (Acesso Múltiplo por Divisão de Código) e, por fim, o mais utilizado, TDMA (Acesso Múltiplo por Divisão de Tempo). Os SDMA separam os canais utilizando antenas direccionais nos leitores ou diminuem a zona de alcance do leitor necessitando assim haver um maior número de leitores: o que torna este protocolo bastante dispendioso. Em relação aos FDMA estes, envolvem a transmissão de dados por parte de uma etiqueta através de um canal de frequência predeterminado, sendo que para isso, a etiqueta deve possuir uma frequência de transmissão livremente ajustável. A alimentação da etiqueta e a transmissão de sinais de controlo realizam-se na frequência adequada f_a. A etiqueta irá responder numa das diversas frequências disponíveis de f_1 a f_N. Os protocolos do tipo CDMA exigem às etiquetas que multipliquem o seu número de identificação único (*Unique Identification* - UID) com uma sequência pseudo-aleatória antes de efectuar a sua transmissão. Este protocolo é eficiente, mas necessitaria de demasiados recursos computacionais para as etiquetas. Este protocolo possui uma grande desvantagem que se prende com o elevado custo dos leitores associados a este género de aplicação. Os protocolos TDMA são os mais utilizados. Estes podem ser divididos em *Tag-Talk-First* (TTF), onde a etiqueta inicia a comunicação com o leitor; e em *Reader-Talk-First* (RTF), caso no qual a etiqueta permanece silenciosa até ser solicitada pelo leitor [53].

No caso de procedimentos do tipo TTF, a comunicação é assíncrona já que não é o leitor a controlar a transferência de dados. Neste tipo de comunicação, o protocolo do género "*Aloha* puro" (e suas variantes) constitui o protocolo mais popular. Neste caso, a etiqueta envia a sua UID ao leitor e espera pela resposta do mesmo. Se esta é positiva, significa que a informação foi bem recebida pelo leitor. No caso contrário, isto é, se a etiqueta recebeu uma resposta negativa, esta indica que ocorreu uma colisão. Para resolver esta problemática, as etiquetas que tiverem recepcionado respostas negativas irão reenviar a sua UID após um atraso temporal aleatório. No caso de procedimentos do tipo RTF, sendo o leitor a iniciar a comunicação, está é do tipo síncrona. E, como podemos observar na figura 18, neste tipo de

comunicação são empregues principalmente três tipos de protocolos (e suas variantes): *Slotted Aloha* (SA), *Framed Slotted Aloha* (FSA) e os protocolos *Tree*. Com o protocolo SA, a etiqueta envia a sua UID em intervalos de tempo síncronos. No caso de ocorrer alguma colisão, a etiqueta retransmitirá a informação após um número aleatório de *slots*. No caso dos protocolos do tipo FSA, estes podem ser divididos em Basic *Framed Slotted Aloha* (BFSA) e *Dynamic Framed Slotted Aloha* (DFSA). Em ambos os casos, cada etiqueta responde uma vez por *frame*. Contudo, com o BFSA, é permitido à etiqueta enviar o seu UID no máximo uma vez por *frame* de tamanho fixo. Com a DFSA, a etiqueta transmite uma vez por *frame*, contudo contrariamente à BFSA, o tamanho da *frame* vária consoante o número de etiquetas presentes [27]. Na tabela 8, é feita uma análise comparativa entre os vários tipos de protocolos *Aloha*.

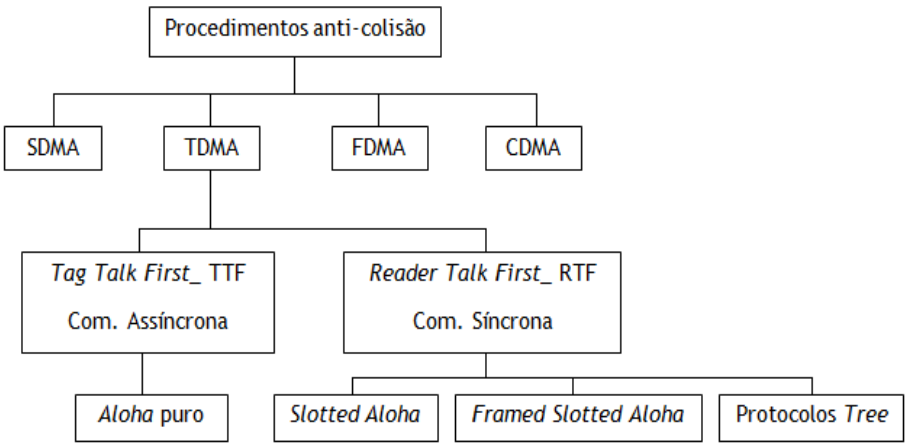
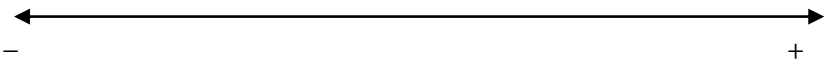
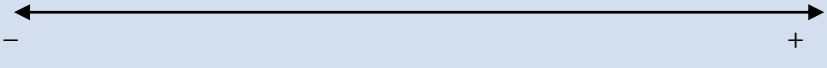


Figura 18: Taxonomia dos protocolos de anti-colisão para sistemas RFID [53].

Tabela 8: Análise comparativa entre os diferentes protocolos de anti-colisão (PA, SA, BFSA, DFSA) [27].

	***Aloha* puro (PA)**	***Slotted Aloha* (SA)**	***Basic Framed Slottet Aloha* (BFSA)**	***Dynamic Franed Slotted Aloha* (DFSA)**
Requisitos necessários à etiqueta	*Timer*	Gerador de números aleatórios, *timer* e circuitos de sincronização	Gerador de números aleatórios e circuitos de sincronização	Gerador de números aleatórios, circuitos de sincronização e nalguns casos gerador de pseudo UIDs
Desvantagens	Aumento do número de colisões com o aumento do número de etiquetas	Aumento do número de colisões com o aumento do número de etiquetas; necessidade de haver sincronização entre o leitor e etiquetas	As etiquetas têm que saber o tamanho da *frame* em utilização; Necessidade de haver sincronização entre o leitor e etiquetas	Monitorização de *slots* sem respostas e requer um receptor sofisticado
Tipo de comunicação	TTF	RTF	RTF	RTF
Custo das etiquetas				
Complexidade do protocolo				

No caso de sistemas que empreguem protocolos do tipo *Tree*, de uma maneira geral, o algoritmo vai dividir as etiquetas que colidiram em "B" subgrupos, sendo "B" um número inteiro maior que 1. Mas, num primeiro passo, o leitor vai comunicar com todas as etiquetas no seu raio de alcance, sendo que cada etiqueta responde à solicitação do leitor gerando um número aleatório. Na figura 19, encontra-se um esquema representativo deste algoritmo. Como podemos observar, baseado no número aleatório de cada etiqueta, estas são separadas em dois subgrupos, sendo B = 2, as etiquetas foram separadas consoante assumiram o número 1 ou 0. Na próxima *slot*, o leitor vai comunicar com as etiquetas do primeiro subgrupo, sendo que se estiver presente no mesmo mais do que uma etiqueta ocorrerá uma colisão. As etiquetas irão então gerar novamente um número aleatório e outros subgrupos serão criados.

Estes procedimentos repetem-se até cada subgrupo ser constituído por uma única etiqueta. Após cada *slot*, o leitor transmite às etiquetas o número de repostas obtidas a cada ronda, para cada etiqueta saber que posição ocupa na "árvore" e quando responder ao leitor [27].

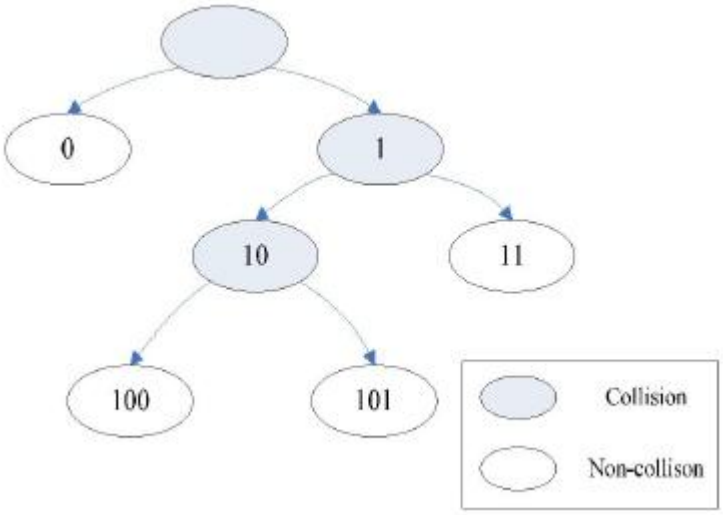


Figura 19: Exemplo do procedimento do algoritmo Tree [54].

3. Módulo TRF7960EVM

Para uma melhor compreensão o funcionamento de sistemas RFID, e de alguns protocolos utilizados, estudou-se o funcionamento do módulo TRF7960EVM, com o objectivo de nos familiarizarmos com a identificação por radiofrequência, trabalhar com alguns protocolos e também adquirir experiência na manipulação de etiquetas.

3.1. Introdução

O módulo de avaliação TRF7960EVM foi concebido com o intuito de ajudar projectistas a avaliar a performance dos múltiplos protocolos por si suportados (ver figura 20). Neste caso foi utilizado o módulo TRF7960EVM (Rev A), produzido pela Texas Instruments.

O módulo opera a uma frequência de 13,56 MHz com a ajuda de uma antena de *loop*, sendo que o processo de leitura das etiquetas é realizado por indução electromagnética. Importa também salientar que, a aplicação de software a ser executada num computador requer um sistema operativo Windows. A ligação entre o computador e o módulo de avaliação é realizada através de uma porta USB padrão.

Foi escolhido este módulo por ser relativamente simples de utilizar e por suportar diversos protocolos, pois trata-se de um software didáctico.

Como foi referido acima, O TRF7960EVM (REV A) fornece suporte para vários protocolos, a saber: ISO 15693, ISO 14443ª, ISO 14443B e Tag-it™ (da Texas Instrument). Para além do mais contém também:

- uma antena incorporada no PCB de 13,56 MHz com a sua respectiva interface electrónica;
- comunicação com a aplicação de software num computador com sistema operativo Windows através de um cabo de USB;
- LED de indicação de protocolo (modo autónomo);
- suporta a comunicação paralela e SPI entre o TRF7960EVM e o MSP430 (configurável utilizando os *jumpers on-board*);
- um MSP430 mais rápido e mais eficiente ao nível energético. O TRF7960EVM utiliza o MSP430F2370 com uma velocidade máxima de relógio de 16 MHz, estando disponível num empacotamento QFN de 40 pinos;
- selecção da fonte de energia através de *jumper*.

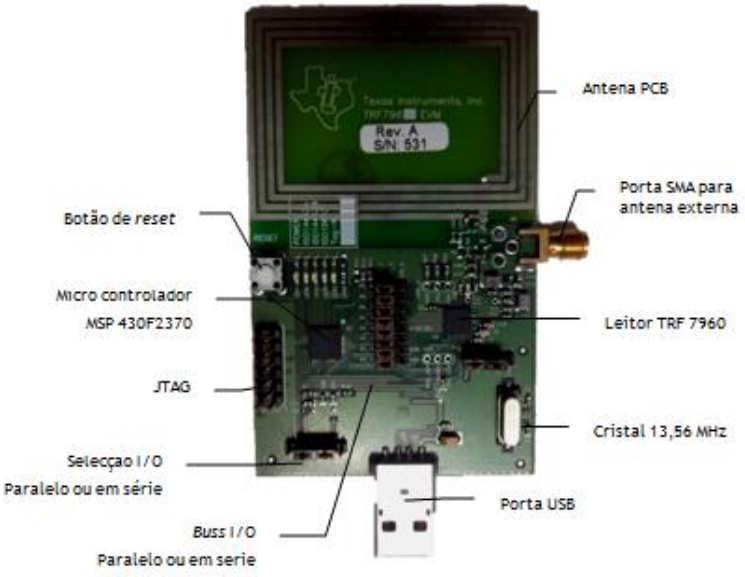


Figura 20: Visão geral do módulo TRF7960EVM (Rev A), visto de cima.

3.2. Interface do software

Após ter instalado correctamente o software, podemos abrir e explorar as capacidades e funcionalidades do equipamento. Na figura 21, podemos observar a janela principal com a descriminação de cada bloco funcional.

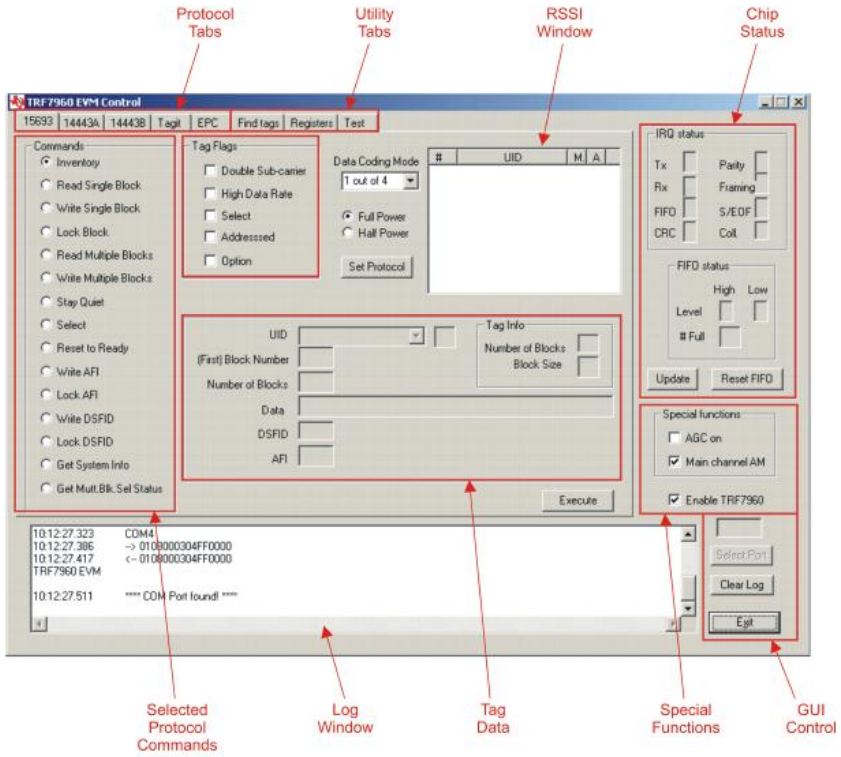


Figura 21: Janela do software com descriminação de cada bloco

3.2.1. Descriminação dos diversos blocos

- **Aba Protocolo:** permite-nos escolher o separador do protocolo com o qual pretendemos trabalhar (ISO 15693, ISO 14443A e B e Tag-it^{Tm}).

- ***Aba Utility*:** os separadores de janelas de utilidades são: "Find Tags" (que permite detectar as etiquetas na zona de leitura do equipamento), "Registers" e "Test".

- ***Aba Flags*:** permite-nos habilitar as opções dos protocolos ISO 15693 e Tag-it^{Tm}. Alguns dos exemplos serão abordados mais à frente.

- ***Chip Status Window*:** disponibiliza-nos informação relativa ao estado em que se encontra o TRF7960EVM.

- ***Command (Request) Window*:** neste bloco temos acesso aos comandos disponíveis para cada protocolo.

- ***Log Window*:** nesta janela são listadas as comunicações realizadas entre o leitor e a etiqueta, incluindo as solicitações. Para distinguir uma da outra, as comunicações feitas a partir da etiqueta aparecem entre parêntesis rectos.

- ***Tag Data Window*:** este bloco permite-nos inserir endereços de etiquetas (i.e. UID), dados, número de bits e outras informações necessárias para executar correctamente alguns comandos.

- ***RSSI Window*:** esta janela exibe o número único de identificação de cada etiqueta, o número de *slot*, e os valores de RSSI (*received signal strength indicator*) que corresponde a um indicador do nível de recepção do sinal. No caso de ocorrer uma colisão, o leitor irá executar um segundo procedimento anti-colisão. O número de *slot* será então identificado com um A no primeiro procedimento, com um B no segundo procedimento, e assim sucessivamente.

Nesta janela, podemos também observar dois canais de RSSI, o AM que constitui o canal principal e o PM que é o secundário. Os valores de RSSI podem variar entre o valor máximo de sete e o mínimo de zero, sendo que estes valores variam com a qualidade da recepção, consequentemente com o design da antena e do leitor. Podemos observar na figura 22 a janela de RSSI.

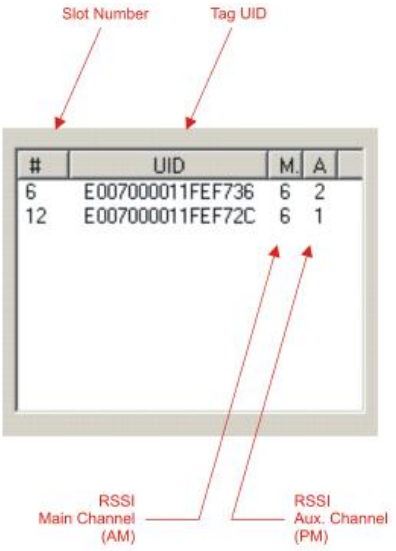


Figura 22: Janela de RSSI

- ***Special Function Window*:** nesta janela podemos encontrar as funções que nos permitem ligar ou desligar o AGC (*Automatic Gain Control*), activar ou desactivar o TRF7960, e passar o canal secundário (PM) de RSSI para principal, quando o valor deste é superior ao valor do canal AM. É importante salientar que, o AGC é desligado após a reinicialização do programa e pode ser ligado sempre que desejado, principalmente em ambientes com ruído.

- **Outras opções/ botões importantes**:

  - ***Set Protocol*:** permite-nos activar o protocolo que foi escolhido previamente no bloco "Selected Protocol Comands".

  - ***Execute button*:** vai iniciar a execução do comando escolhido.

  - ***(Output) Power Control*:** pode ser configurado para "*Half-Power*" (200mW) ou "Full-Power" (100mW), sendo este último o nível mais eficiente. Esta opção permite-nos simular condições marginais de recepção.

3.2.2. Noções importantes

Para uma correcta utilização desta aplicação de *software* é necessário ter em mente duas ideias essenciais:

- no protocolo ISO 15693 é necessário que a opção "Option", na janela "tags flag", esteja a 1 para se poder utilizar todos os comandos de escrita e de "lock" correctamente;

- O número de blocos pode ir de 0 até 255, isto é, de 0x00 até 0xFF em hexadecimal. É importante ter em atenção que, quando falamos em 0x03, por exemplo, na realidade estamos a falar de 4 blocos, pois 00 também constitui um bloco.

3.2.3. "Find Tags"

A janela "Find Tags", como o seu nome indica, permite-nos detectar as etiquetas que estão ao alcance do leitor. Dessa maneira, o leitor envia um pedido de inventário que será recebido pelas etiquetas.

Como podemos observar na figura 23, as opções desta janela permitem ao utilizador escolher os protocolos com que pretende trabalhar. Para isso deve seleccionar e configurar adequadamente os campos correspondentes ao(s) protocolo(s) pretendido(s).

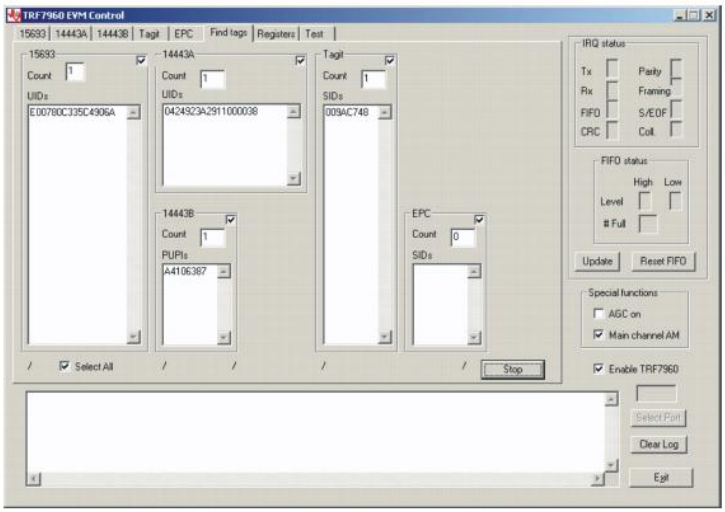


Figura 23: Janela "*Find Tags*"

Para iniciar a procura de uma etiqueta é necessário executar o comando "Run", sendo que os UID das etiquetas encontradas aparecerão na janela do protocolo suportado. Para parar a procura, é necessário executar o comando "Stop".

3.3. ISO/IEC 15693

Neste sub-capitulo serão descritos os comandos relativos ao protocolo ISO 15693. Na figura 24, podemos observar a janela relativa aos comandos e as opções relativa às etiquetas utilizando a norma ISO/IEC 15693.

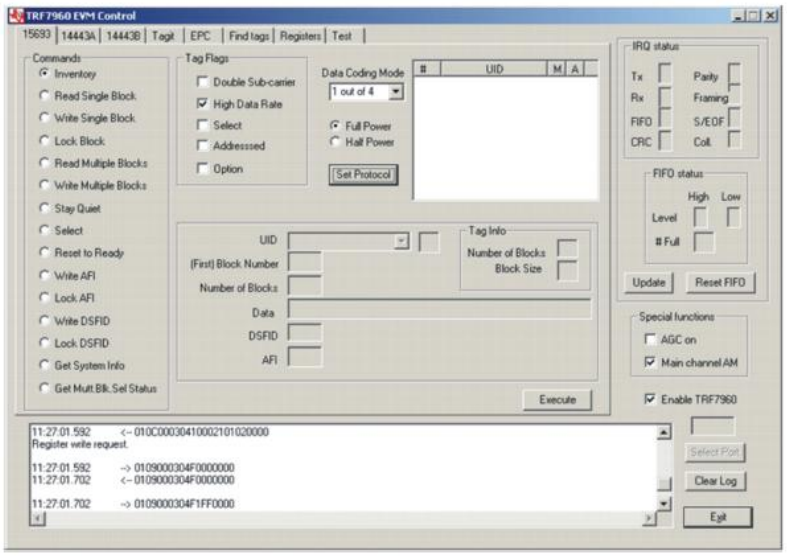


Figura 24: Janela do protocolo ISO 15693.

Qualquer comando do protocolo ISO 15693 estabelecido envia três operações: escrita no registo, estabelecimento do AGC (*Automatic Gain Control*) e activação do modo de receptor (AM/PM). De seguida são descritos os endereços de solicitação de cada comando, com o respectivo conteúdo de cada um deles.

1. Escrever no registo:

Tabela 9: Endereço de solicitação para escrita no registo.

Endereço de solicitação		
Campo	**Valor**	**Observações**
SOF	0x01	Início da *frame*
Tamanho dos pacotes(dados)	0x0C	Tamanho = 12 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando *Firmware*	0x10	Escrita no registo
Registo 0x00	0x00 0x21	No registo 0x00, *chip status control register*, escreve 0x21 que vai activar as saídas RF com uma corente contínua de 5V
Registo 0x01	0x01 0x02	No registo 0x01 *ISO control register*, escreve 0x02 (protocolo definido para alta taxa de bits do protocolo ISO 15693, 26,46kbps, 1 de 4
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010C0003041000210102000**0		

2. Estabelecer o AGC: ver tabela 10.
   Tabela 10: Endereço de solicitação para estabelecimento do AGC.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
SOF	0x01	Início da *frame*
Tamanho do pacote (dados)	0x09	Tamanho do pacote = 9 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando de *firmware*	0xF0	AGC comuta
AGC Off	0x00	AGC On = 0xFF
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **0109000304F0000000**		

3. Habalitação do modo de receptor (AM/PM): a tabela contendo o endereço de solicitação para habilitação do modo receptor, encontra-se na tabela B.1 anexo B.

3.3.1. Comandos do protocolo ISO/IEC 15693

Para o protocolo ISO 15693 este módulo suportada as seguintes funcionalidades:

Inventory - utilizado para adquirir o UID (*Unique Identifacation*). O inventário pode ser feito de duas maneiras diferentes: "*single-slot*" e "16-*slotted*". Na primeira, todos as etiquetas podem responder ao pedido de inventário, sendo que, no caso de haver mais do que uma etiqueta na zona de leitura, ocorrerá uma colisão de dados. Com o segundo método, a probabilidade de colisão é significativamente menor. Neste mecanismo os *transponders* podem responder em uma das 16 *slots*. No anexo B, encontra-se a tabela 2 com o endereço de solicitação do comande de inventário.

Read Single Block - leitura de um único bloco; este comando permite-nos ler os dados de um único bloco da memória da etiqueta, assim como saber se este se encontra

protegido ou não contra a escrita. O endereço de solicitação e o código de resposta a este comando encontram-se nas tabelas 3 e 4 do anexo B, respectivamente.

Write Single Block - escrita de um único bloco; este comando permite escrever dados num único bloco da memória da etiqueta. Para efectuar a operação com sucesso, o utilizador terá que estar ciente do tamanho da memória do bloco em que pretende escrever. Esta informação encontra-se disponível através do comando "Get System Information Request". É importante ter em atenção que, no protocolo ISO 15693 é necessário na janela "tags flag" colocar a opção "Option" a 1 para se poder utilizar todos os comandos de escrita e de "lock" correctamente. A tabela com o endereço de solicitação deste comando encontra-se na tabela 5 do anexo B e a resposta da etiqueta a esta solicitação está na tabela 6.

Lock Block - proteger um bloco único contra a escrita. Como já foi referido anteriormente, é importante ter em atenção que, no protocolo ISO 15693 é necessário a opção "Option" na janela "tags flag" estar a 1 para se poder utilizar todos os comandos de escrita e de "lock" correctamente. No anexo B, nas tabelas 7 e 8, encontra-se o endereço de solicitação que permite proteger um bloco de memória da etiqueta contra a escrita e resposta da etiqueta à solicitação do comando "Lock Block".

Read Multiple Blocks - leitura de vários blocos; este comando permite-nos obter os dados de diversos blocos para além de, nos facultar o estado de segurança de cada bloco, como por exemplo, se se encontra bloqueado, aberto à escrita, etc.

Write Multiple Blocks - escrita de vários blocos; este comando permite-nos escrever em diversos blocos específicos da memória das etiquetas que se encontram na zona de leitura do equipamento. Tal como para a escrita de um único bloco, para utilizar este comando de maneira correcta é necessário conhecer o tamanho de memória de cada bloco da etiqueta. Podemos consultar esta informação através do comando "Get System Information". Assim, podem ser encontradas no anexo B, as tabelas 9 e 10 contendo o endereço de solicitação para escrita de múltiplos blocos e a resposta da etiqueta a esta mesma solicitação, respectivamente.

Stay Quiet - silenciar etiquetas; esta funcionalidade permite-nos fazer com que uma etiqueta não responda a qualquer comando ou inventário, a não ser que o número de UID seja correspondente. A tabela 11 do anexo B contém o endereço de solicitação do comando "Stay Quiet", sendo que a tabela 12 contém a resposta da etiqueta a este comando.

Select - seleccionar etiqueta; este comando coloca a etiqueta no modo "seleccionado". Nesta condição, a etiqueta é directamente controlado através do campo "<IsSelectMsg>", presente nas mensagens de solicitação dos diversos comandos do protocolo ISO 15693. Qualquer etiqueta que se encontre no modo seleccionado, e que receba uma

solicitação, na qual o UID não seja correspondente, entrará em modo ”Ready”, mas não enviará nenhuma resposta. No anexo B podemos encontrar, na tabela 13, o endereço de solicitação para este comando. A resposta da etiqueta a esta solicitação encontra-se na tabela 14 desse mesmo anexo.

Reset to ready - coloca as etiquetas desejadas novamente em estado activo. Neste modo, a etiqueta não responde às solicitações em que a *flag* “Select” do protocolo de comunicação ISO 15693 se encontra habilitada, mas sim a todo e qualquer pedido, mesmo que não seja endereçada especificamente, desde que a solicitação tenha o mesmo UID. De certa forma, este comando é complementar ao comando “Select”, anulando-o. Podem ser encontrados os endereços de solicitação deste comando e a respectiva resposta da etiqueta nas tabelas 15 e 16 do anexo B.

Write **AFI** (*Aplication Family Identifier*) - grava um novo valor no registo AFI da etiqueta endereçada. Sendo que, a “Aplication Family Identifier” o tipo de aplicação em que a etiqueta é empregue. Esta é utilizada para extrair informações de etiquetas que satisfazem as necessidades da aplicação. No anexo B a tabela 17 e a tabela 18, descrevem o endereço de solicitação do comando “*Write* AFI” e a resposta da etiqueta.

Lock **AFI** - protege o registo AFI, das etiquetas endereçados, contra a escrita. O endereço de solicitação do comando “Lock AFI” encontra-se na tabela 19 do anexo B e a resposta da etiqueta a este comando aparece na tabela 20 desse mesmo anexo.

Write **DSFID** (*Data Storage Format* identification) - escreve um novo valor no registo DSFID da(s) etiqueta(s) endereçada(s). No anexo B, mais precisamente nas tabelas 21 e 22, encontram-se o endereço de solicitação deste comando e a resposta da etiqueta à solicitação deste comando, respectivamente.

Lock **DSFID** - protege o registo DSFID das etiquetas endereçadas contra a escrita. Assim, podem ser encontradas no anexo B as tabelas 23 e 24 contendo o endereço de solicitação deste comando e a resposta da etiqueta a esta mesma solicitação, respectivamente.

Get System Info - recupera informações da etiqueta tais como: identificação, família de aplicações, formatação de dados, tamanho do bloco de memória conforme especificado pelo protocolo ISO 15693. O endereço de solicitação que recupera a informação da etiqueta e o código de resposta a este comando encontram-se nas tabelas 25 e 26 do anexo B, respectivamente.

Get multiple Block Secuity Status - Coloca blocos de bytes em modo de segurança. Este comando faz com que seja atribuído um byte de segurança para cada bloco que desejamos bloquear. Por outras palavras, este byte codifica a protecção contra a escrita do bloco desejado. Podem ser encontrados o endereço de solicitação deste comando e a respectiva resposta da etiqueta nas tabelas 27 e 28 do anexo B.

3.4. Janela "Test"

Esta janela permite-nos introduzir manualmente os comandos utilizando a aba "test". Para isso, basta introduzir o comando e parâmetros desejados (no formato hexadecimal) nas linhas de campo correspondentes. Na tabela 11, podemos encontrar alguns exemplos, sendo que, o sexto byte corresponde ao código do comando, seguido pelo código dos parâmetros. A comunicação acaba com dois bytes de 0x00.

Tabela 11: Exemplo de códigos de comandos e parâmetros.

Comando	Parâmetros	Exemplo
0x03 Activar/desactivar o módulo	0x00 - Activar leitor 0xFF - Desactivar leitor	01 09 00 03 04 **03 FF** 0000
0x0F Modo directo		01 08 00 03 04 **0F** 0000
0x10 Escrever registo único	Endereço, dados, endereço, dados, …	01 0A 00 03 10 **15** 67 0000
0x11 Escrita contínua	Endereço, dados, dados,…	01 0C 00 03 04 **11** 13 67 46 A4 0000
0x12 Ler registo único	Endereço, endereço, …	01 0B 00 03 04 **12** 01 0A 13 0000
0x13 Leitura contínua	Nº de byte a aceder, endereço inicial	01 0A 00 03 04 **13** 05 03 0000
0x14 Inventario (ISO 15693)	Dados FIFO	01 0B 00 03 04 **14** 06 01 00 0000
0x15 Comando directo	Código do comando directo	01 09 00 03 04 **15** 0F 0000
0x16 Escrever uma coluna	Dados ou comandos	01 10 00 03 04 **16** 91 3D 00 40 AA BB CC DD 0000
0x18 Comando de solicitação	*Flags*, código do comando, dados, …	01 0B 00 03 04 **18** 06 20 01 0000
0xF0 Selecção do AGC	0x00 - Activar AGC 0xFF - Desactivar AGC	01 09 00 03 04 **F0** FF 0000
0xF1 Seleccionar AM/PM *input*	0x00- Input FM 0xFF-Input AM	01 09 00 03 04 **F1** 00 0000

4. Avaliação das actividades hospitalares com potencial de aplicabilidade da tecnologia RFID

Em meio hospitalar, a ocorrência de erros no decorrer do internamento pode, na maior parte dos casos, levar a um aumento considerável dos custos com a saúde. Para além do que o mais pequeno erro pode fazer toda a diferença entre a vida e a morte [55].

A HealthGrades, uma organização de saúde Norte Americana, realizou um estudo referente aos anos 2000, 2001 e 2002, no qual demonstrou que nos Estados Unidos da América morreram, em média, 195 000 pessoas por ano em consequência de erros que podiam ter sido evitados [56]. Do estudo resultou a conclusão de que este problema não se deve à falta de qualificação do pessoal de saúde, mas sim, a factores como: más condições de trabalho, situações de stress, descuidos vários, excesso de trabalho, e cansaço [57].

A constatação do estudo anterior tem levado as equipas de investigação a analisar esta problemática. Em consequência destes trabalhos, têm sido propostas novas tecnologias com o intuito de permitir a automatização de diversos procedimentos hospitalares. Pretende-se desta forma diminuir as probabilidades de erro. Algumas das tecnologias propostas têm como base os sistemas de código de barras ou as tecnologias RFID. A identificação por radiofrequência apresenta um potencial de aplicabilidade maior, quando comparada com as outras, já que possui maior fiabilidade, eficiência e versatilidade. O potencial de aplicabilidade das tecnologias RFID em tarefas como o rastreamento de objectos ou de pacientes, e o apoio à realização de inventários, entre outras aplicações, será discutido mais à frente neste capítulo [58, 59].

4.1. Melhoria da segurança dos pacientes

Em ambiente hospitalar, a segurança dos pacientes pode ser aumentada reduzindo erros e melhorando a segurança. Os erros podem ter diversas origens. Podem ocorrer erros na admissão do paciente, ou até pode acontecer que seja aplicado o tratamento errado ao doente, sendo que alguns destes erros podem ter consequências graves na sua saúde, ou inclusivamente provocar a sua morte.

4.1.1. Identificação e rastreamento dos pacientes

A identificação errónea de um paciente pode ter consequência (graves) na sua saúde, tais como, levar a uma incorrecta administração de medicamentos, a um procedimento (endoscopia, cirurgia entre outras) invasivo indevido, atribuição de exames de imagiologia ou laboratoriais à pessoa errada o que consequentemente pode desencadear um diagnóstico incorrecto, induzindo directamente em mais erros médicos [56].

Na ausência de tecnologias de identificação automática, a recolha de dados relativamente a um paciente é, geralmente, feita à mão e armazenada em papel. Esta informação necessita ser actualizada ao longo do processo terapêutico, como por exemplo, para descrever os procedimentos utilizados ou a medicação prescrita. Este método, por ser realizado manualmente, possui um vasto leque de inconvenientes, tais como: demora na actualização dos dados e dificulta o seu acesso. Mas, talvez o maior inconveniente é que pode conduzir facilmente a erros médicos. Na identificação automática, que tem por base a tecnologia RFID, aquando da chegada do doente ao hospital é-lhe atribuído um número único de identificação (UID). O UID é programado numa etiqueta de RFID, embutida numa pulseira colocada no paciente. É importante salientar que os dados contidos na etiqueta estão protegidos com palavra passe, garantindo-se assim a privacidade e o sigilo médico. Para além de identificar o paciente de forma segura, podem ser introduzidas informações adicionais importantes, tais como, grupo sanguíneo, alergias, medicamentos prescritos e outras informações relevantes, facilitando e acelerando assim os procedimentos médicos. Outra vantagem deste sistema é a possibilidade de consultar e actualizar a ficha do paciente via *Wi-Fi* através de um PDA, telemóvel ou computador [39, 60].

Neste contexto, e com o objectivo de melhorar os cuidados médicos e evitar os erros médicos, sobretudo na sala de operações, a Aionex criou o SkyeTek, que tem por intuito identificar de forma segura e fiável a identidade do paciente. Este sistema utiliza etiquetas de RFID passivas e leitores normalizados com os protocolos ISO 15693, ISO 14443A e ISO 18000-3, conjuntamente com uma impressora de etiquetas RFID. Quando o paciente chega ao serviço de cirurgia, a sua etiqueta de RFID já contém o seu UID, que está associado ao seu ficheiro na base de dados da Aionex. A etiqueta é aplicada no local do corpo onde a cirurgia deverá ser efectuada. No período pré-operatório, a enfermeira faz uma leitura da etiqueta, sendo que as informações associadas ao UID, tais como: identidade do paciente, local a ser operado, tipo de cirurgia e outras informações importantes são passíveis de serem exibidas num computador pessoal, num PDA ou num ecrã presente na sala de operações. A informação disponível pode ser consultada a qualquer momento [61].

O módulo associado a esta aplicação é o SkyeModule™ M1, apresentado na figura 25. Este módulo é do tipo OEM (*Original Equipment Manufactures*) múltiprotocolos que opera a uma frequência de 13,56 MHz. E, capaz de ler e escrever em etiquetas que obedeçam às normas ISO 15693, ISO 14443A e ISO 18000-3. O SkyeModule™ M1 possui uma antena própria, mas pode-lhe ser adicionada uma antena externa, com uma impedância de 50 Ohm, para aumentar o seu alcance de leitura. Em relação à comunicação com o *host*, esta pode ser realizada através de 4 interfaces diferentes: RS232, UART serial, I2C e SPI. Este módulo possui um circuito regulador de tensão, e pode por isso ser alimentado com uma tensão entre os 1,8 V e os 5 V. A corrente requerida pelo seu funcionamento é de 60 µA em modo de suspensão. O SkyeModule™ M1 possui também 8 GPIO (*General Purpose Input/output*) na eventualidade de ser necessário adicionar dispositivos periféricos. Para além de todas estas funcionalidades, o SkyeModule™ M1 é de pequenas dimensões e preço reduzido, sendo que é utilizado por exemplo pela tag-it da Texas instruments [62].

Em relação ao rastreamento dos doentes, a Clarinox Tecnologies desenvolveu um sistema baseado nas tecnologias RFID e RTLS (*Real Time Localization System*) que nos permite identificar e localizar pacientes em tempo real. Desta feita, criou o Clarinox WayPoint. O sistema divide a zona a cobrir em diferentes áreas, sendo que, cada área possui a sua própria estação de base. Essa estação recebe os sinais enviados pelas etiquetas presentes no espaço, de seguida guarda-os e processa as informações contidas nas etiquetas. Toda a informação relativa ao sistema é administrada a partir de um único computador que possui um sistema operativo Windows da Microsoft. Na figura 26, encontra-se um esquema ilustrativo do funcionamento deste sistema de localização em tempo real [63].

Figura 25: Fotografia do módulo 1 da SkyeTek [63].

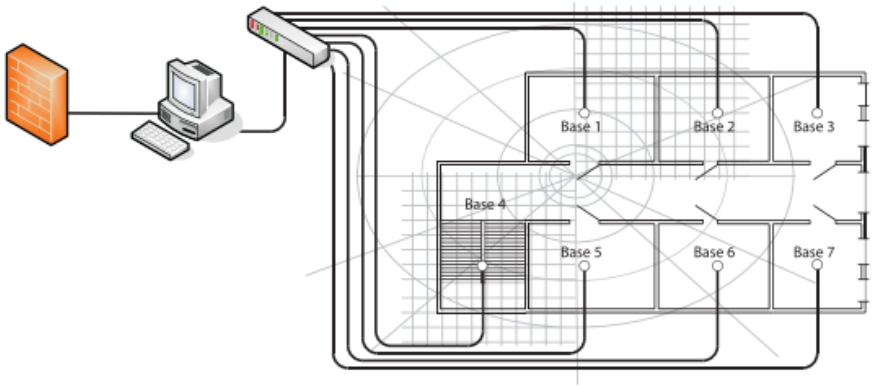


Figura 26: Esquema ilustrativo do funcionamento deste sistema RSTL [64].

A Clarinox Waypoint possui outro sistema RFID, desta vez do tipo activo, que opera numa frequência de 2,4 GHz: o Clarinox Yulo. Este sistema suporte dois tipos de etiquetas a nano-tag Yulo e a micro-tag Yulo. A primeira possui menores dimensões (24x20x6 mm), um menor tempo de vida útil de aproximadamente um ano. Não pode ser associada a um sensor, sendo que a micro-tag Yulo pode ser usado como sensor de temperatura e efeito de Hall. Esta segunda etiqueta, como já foi referido, possui dimensões maiores (58x35x16 mm), e incorpora uma bateria com um tempo de vida útil de aproximadamente quatro anos. Em relação ao leitor, este requer uma alimentação de +5 VDC e possui um alcance de leitura de 20 a 30 m em interiores, e de 30 a 80 m em campo aberto. Existem dois modelos disponíveis: o leitor Yulo USB e o Leitor Yulo Ethernet. A principal diferença entre os dois consiste no seu modo de alimentação, sendo que o primeiro obtém-na de uma bateria e o segundo a partir de um adaptador de 5V a 140 mA [65].

Existem outras empresas que disponibilizam aplicações e produtos capazes de identificar o paciente e/ou sua localização em tempo real, entre as quais destacamos: a Awarepoint, a PURELINK Technology, e a Exavera. Estes produtos serão abordados mais à frente neste capítulo.

Assim podemos concluir que, a identificação por radiofrequência é uma tecnologia ainda em pleno crescimento, porém, já nos permite não só identificar em tempo real de forma fácil, eficaz e segura um paciente, mas também permite conhecer a sua localização [66]. Os sistemas RFID permitem assim processar e consultar informações médicas acerca do paciente de modo simples e seguro [61].

4.1.2. Segurança dos recém-nascidos

Outro domínio em que a tecnologia RFID aumenta de forma clara a segurança dos pacientes é no caso dos recém-nascidos. Este objectivo pode ser alcançado evitando a entrega de bebés aos pais errados e prevenindo os raptos. Regra geral, os hospitais atribuem as causas destes incidentes a erros humanos: má leitura da pulseira do bebé ou da mãe, queda e/ou perda da pulseira dos recém-nascidos, troca de berços, troca de bebés com nomes semelhantes, entre outras. [67]

Em Portugal, esta implementação já foi aceite e reconhecida, sendo que a partir de 2009, tornou-se aconselhado o uso de pulseiras embutidas com etiquetas de RFID nos recém--nascidos em todos os serviços de Obstetrícia, Neonatologia e Pediatria [68].

Aquando do nascimento, duas etiquetas idênticas são geradas por um leitor/programador de RFID, sendo uma inserida na pulseira da mãe e outra na do bebé. Aquando da saída, os UID da pulseira de mãe do seu recém-nascido são comparadas pela aplicação de software. Se forem correspondentes podem então sair, se não, o número da pulseira do bebé em falta é procurado através do sistema de RFID e aparecerá no mapa. Após a alta da mãe e do seu bebé, as etiquetas são reprogramadas e reutilizadas, o que torna a sua utilização mais rentável. É importante salientar que, essas pulseiras são invioláveis e à prova de falsificação, assim sendo, se alguém tentar retira-la sem autorização, se cair ou se o recém-nascido é retirado sem autorização do berçário, é de imediato activado um alarme e as portas da unidade serão enceradas [69-71].

Um bom exemplo prático é o BlueTag produzido pela Logicpulse. Este sistema é composto por uma etiqueta activa que opera em UHF, possuindo uma bateria com duração de 18 meses, que envia sinais a cada segundo. Para aumentar a segurança deste sistema, as etiquetas possuem um aviso de bateria fraca e, para o caso de cortes energéticos, o posto de controlo está equipado com discos redundantes e alimentação de emergência. A aplicação de software associada é de utilização simples, sendo que, a partir de um computador, entre outras funcionalidades podem ser realizadas as associações das etiquetas entre a mãe e o recém-nascido; ou a gestão das saídas provisórias ou definitivas. O sistema BlueTag é caracterizado por utilizar dois tipos de leitores: leitores de longo alcance utilizados para cobrirem uma grande área, até aproximadamente 30 metros; e os leitores de curta distância, localizados perto dos acessos, possuindo um alcance de leitura ajustável que pode variar dos 3 aos 15 metros. É também importante salientar que os leitores se encontram interligados, com alimentação própria e ligados a um alarme próprio. Este sistema é igualmente utilizado com doentes que sofrem de Alzheimer, doentes psiquiátricos ou que apresentem algum risco de fuga ou de se perderem no hospital [70, 72].

O Safe Place®, criado pela RFTechnologies, é outro sistema RFID para protecção e segurança dos bebés, lançado com sucesso no mercado. Apesar da BlueTag"e o Safe Place terem o mesmo princípio de funcionamento, tais como: braceletes invioláveis ou alarmes que bloqueiam as portas, estes sistemas apresentam todavia diferenças a nível operacional. O Safe Place® possui transmissores de dupla frequência: 262 kHz e 318 MHz. Os sinais enviados na frequência de 262 kHz são captados pelos leitores localizados junto das portas de saída e elevadores, sendo que, os leitores espalhados pelo serviço recolhem os sinais na frequência dos 318 MHz. Outra diferença encontra-se no facto de que, as etiquetas do Safe Place® enviam sinais ao leitor em intervalos de 10 segundos [73].

Na tabela 13 encontram-se sumarizadas as principais diferenças de funcionamento entre o BlueTag e o Safe Place®.

Tabela 12: Diferenças entre o sistema BlueTag e Safe Place® [72, 73].

	Tipo de etiqueta	Frequência de funcionamento	Envio de sinal	Curiosidades
BlueTag	Activa	UHF	A cada segundo	Implementada numa dezena de países
Safe Place®	Activa	262 kHz e 318 MHz	A cada 10 s	Possui serviço de monitoramento remoto

Outra empresa que se debruçou sobre este assunto foi a Intel Corporation em parceria com a ECO Inc. e o Wonju Christian Hospital. O sistema desenvolvido por esta pareceria possui um funcionamento basicamente semelhante aos anteriores. Porém, apresenta uma inovação, já que permite a partilha de dados com as famílias dos bebés. Para esse efeito encontra-se instalado um quiosque na entrada da área restrita onde se encontram os bebés. Nesse quiosque encontram-se inseridas, para cada bebé, a sua fotografia e a informação médica acessível, como: altura; peso: temperatura; e outras informações consideradas pertinentes. Para poderem aceder aos dados do seu bebé, os familiares têm que introduzir o número de identificação da mãe no quiosque. Na figura 27 apresenta-se a imagem dum quiosque utilizado nesta aplicação. Este sistema, contrariamente ao BlueTag, utiliza etiquetas passivas de 1024-bit que seguem a norma ISO 15693, operando à frequência de 13,56 MHz, utilizando leitores com um alcance máximo de leitura de 50 cm à frequência de 13,56 MHz [74].

Figura 27: Imagem de um quiosque utilizado na entrada da área restrita da neonatologia [74].

4.1.3. Gestão da farmácia e dos medicamentos

Os erros envolvendo a administração de medicamentos podem ocorrer aquando da sua prescrição, da execução da receita, da sua administração ou com o fim da validade dos medicamentos [75]. Assim, para auxiliar as enfermeiras, foi instituído o método dos cincos "certos" para administração de medicação. Estas têm que se certificar que estão a tratar: o paciente certo, com a medicação certa, com a dosa certa, pela via certa e à hora certa. Apesar desta ajuda, e porque os enfermeiros trabalham sob grande pressão, os erros continuam a acontecer [76, 77].

Na área da gestão das farmácias hospitalares, a identificação por rádio frequência também é adequada à simplificação do trabalho do pessoal de saúde, contribuindo para o aumento da segurança dos pacientes. A utilização desta tecnologia possibilita o controlo, a gestão e a fiscalização dos medicamentos, assegurando sua correcta administração ao paciente [78].

Com o intuito de resolver esta problemática foi criado o *Inpatient Safety RFID System* (IS-RFID). Este sistema utiliza etiquetas passivas do tipo EPC Gen-2 (ver Anexo A), com uma *password* de 32-*bits*, possuindo uma função de PRNG (*Pseudo-Random Number Generator*), isto é, um gerador de números pseudo-aleatórios de 16-bit. Em relação aos leitores e PDA, estes têm que estar ligados à base de dados através de uma ligação autenticada e encriptada por motivos de segurança. Ao visitar um paciente, o médico, auxiliado pelo seu PDA, vai ler as informações contidas na etiqueta de RFID da sua pulseira, evitando desde logo uma má identificação do paciente. No fim da consulta, se houver necessidade de alterar a medicação ou de efectuar uma nova prescrição, o médico introduz as alterações no seu PDA. No final das consultas descarregará os dados para o seu PC, ligado ao sistema de informação do hospital

(SIH). De seguida, o SIH informa a farmácia onde serão preparadas as receitas, sendo que os medicamentos de cada paciente são colocados num saco de plástico. Os medicamentos contidos em cada um dos sacos são agrupados em tuplos. Feito isto, é gerada uma identificação (UID_i) para cada uma das bolsas, que será embutida numa etiqueta passiva que depois será, por sua vez, colocada na sua respectiva bolsa. Para finalizar o processo, a identificação de cada pacote de medicamentos é introduzida na SIH. De seguida, é enviado para cada andar um carinho com a medicação destinada aos internados nesse piso. Depois de receber o carinho, uma enfermeira vai ligar-se ao SIH e requisitar as informações relativas aos medicamentos que recebeu. O SIH envia os tuplos que se apresentam da seguinte maneira (ver tabela 13):

Tabela 13: Tabela representativa da informação contida nos tuplos [79].

$Paciente_1$	UID_1	t_1	$Informação\ adicional_1$
.	.	.	.
.	.	.	.
.	.	.	.
$Paciente_N$	UID_N	t_N	$Informação\ adicional_N$

Assumindo que um andar tenha N pacientes, vem então uma listagem com N tuplos, sendo que em cada um deles aparece a identificação do paciente, a identificação da embalagem relativa ao paciente, a hora (t) em que devem ser administradas e, por fim, nas informações adicionais podem constar dados como: modo de administração do medicamento, dosagem ou um *link* para o ficheiro do paciente. De seguida, a enfermeira transfere os dados para o seu PDA e já pode iniciar a ronda para administração dos tratamentos. Ao chegar ao paciente, o primeiro passo é verificar que a identidade do paciente e da embalagem contendo os medicamentos correspondem. Para isso, o leitor (PDA) gera um número aleatório que envia com uma mensagem de solicitação (r_s) para a etiqueta da pulseira do paciente e a da embalagem que contém os medicamentos. Cada uma das etiquetas, após ter recebido o sinal, gera o seu próprio número aleatório e outro número criado através de um gerador de número pseudo-aleatórios (PRNG). Relativamente à etiqueta do paciente, o número gerado é composto pela combinação do número do paciente ($Paciente_x$), com o r_s, com o número gerado pela própria etiqueta (r_p). No caso da etiqueta da embalagem, o número gerador provém da combinação do UID, com o r_s, com o número gerador pela própria etiqueta (r_e). A junção desses dois números consiste na mensagem de respostas das etiquetas ao leitor PDA:

- Resposta da etiqueta do paciente: $\{r_p, PRNG(Paciente_x, r_s, r_p)\}$;
- Resposta da etiqueta da embalagem: $\{r_e, PRNG(UID_x, r_s, r_e)\}$.

Após ter recebido a resposta das duas etiquetas, o PDA vai associar o número do paciente com o UID da embalagem $\{paciente_x, UD_x\}$, e de seguida vai gerar os seus {PRNG

(paciente$_x$, r_s, r_p), PRNG (UD$_x$, r_s, r_e)}. Se o valor gerado pelo PDA é igual ao guardado, aparecerá então no ecrã uma mensagem de confirmação. Consequentemente é gerado um registo. A enfermeira pode então administrar os medicamentos ao paciente em segurança. Aquando da correcta administração, a enfermeira a partir do seu PDA acede a janela "tempo" especificada pela SIH e procede novamente à leitura das duas etiqueta para ficar registado a correcta administração e a hora a que esta ocorreu. Para finalizar o procedimento, após ter administrado os medicamentos a todos os pacientes, a enfermeira volta ao computador onde acede ao SIH e descarrega as informações contidas no seu PDA. O SIH verifica a validade das informações recebidas e se estas foram correctamente introduzidas na janela "tempo". No caso de se detectar alguma anomalia, um alarme é accionado e um procedimento de má administração de medicamento é lançado [79].

4.1.4. Sistema de gestão de amostra para laboratório

Nos laboratórios de análises clínicas, a correcta rotulagem e identificação dos frascos contendo as amostras biológicas dos pacientes é outra área crítica onde os erros podem desencadear um diagnóstico erróneo. Consequentemente pode levar a um tratamento inapropriado que, a ser realizado, pode ter consequências fatais para o paciente. Estes erros podem ser de dois tipos: má identificação do paciente (amostra rotulada com nome ou número de identificação do paciente errado) ou má identificação da amostra (má identificação da origem e da hora da colheita) [80].

Com o intuito de evitar estes erros médicos e de tornar esse processo seguro, a Maxell criou a etiqueta Coil-On-Chip™ que é embutida na base dos tubos de ensaios para amostras, como podemos observar na figura 28 [81].

Figura 28: Tag Coil-On-ChipTM embutida em tubos de ensaio [82].

Esta etiqueta, do tipo leitura/escrita (*read/write*), consiste numa antena directamente montada num *chip* com uma área de 6,25 mm^2. Em relação à memória da

etiqueta, consoante o modelo, pode ir dos 128 bytes aos 4 kbytes. Esta permite o armazenamento de várias informações, tais como: a identificação do paciente, a identificação e o histórico da amostra (origem e testes efectuados na mesma). As especificações detalhadas do Coil-On-Chip™ encontram-se no anexo C. Contudo, é importante salientar que o Coil-On-Chip™ opera através de um protocolo também criado pela Maxell. Em relação ao leitor, a Maxell dispõe de vários modelos, consoante as especificidades que se pretende implementar na aplicação, tais como, interface com o *host*, alcance de leitura, consumo de energia, número de antenas, entre outros. Cada leitor detecta 48 tubos de cada vez, sendo esta a quantidade máxima de tubos que pode conter o suporte de tubos [83]. Na figura 29 encontra-se um leitor com o seu suporte.

Figura 29: Leitor/ impressora com o suporte para os tubos [84].

O sistema Coil-On-Chip™ é fornecido com a aplicação de software. Como se pode observar na figura 30, esta é de simples utilização, sendo que contém a imagem do suporte dos tubos com as devidas legendas, as teclas para os comandos (procura, leitura, escrita). Na parte inferior da janela da aplicação estão representados os dados referentes ao tubo da linha seleccionada.

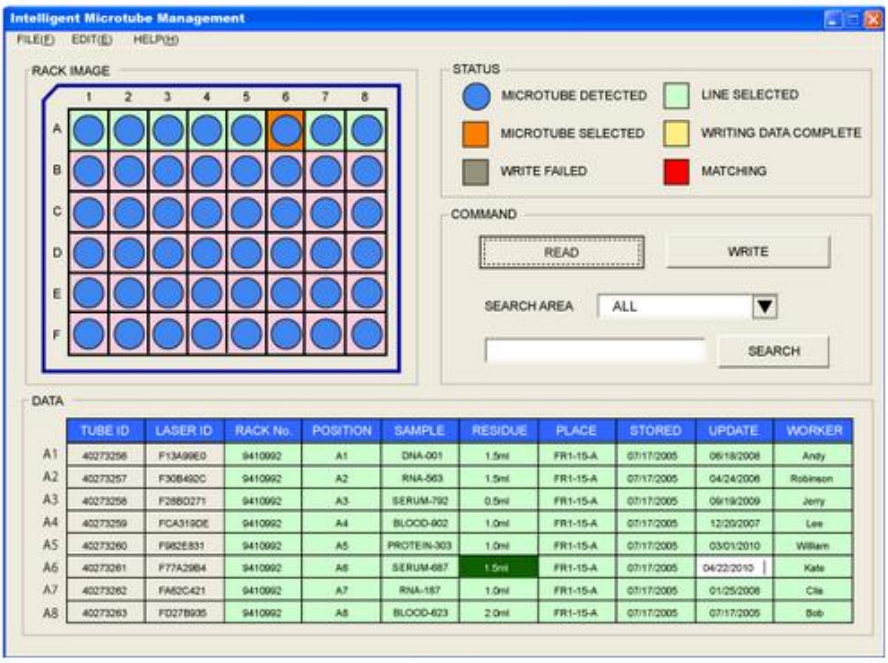


Figura 30: Display da janela principal de aplicação do software Intelligent Microtube Managment da Maxell Seiki, ltd [84].

A segurança dos dados é garantida através de procedimentos de encriptação. Por outro lado, o alcance de leitura é extremamente reduzido contribuindo também para a segurança dos dados contra acessos indevidos [84].

4.1.5. Corpos estranhos retidos

A cirurgia tem evoluído muito nos últimos anos, sendo que o uso da alta tecnologia e das ferramentas é actualmente bastante comum, tornando esta especialidade cada vez mais segura. No entanto, casos de esquecimentos de utensílios no corpo do paciente são denominados por "corpos estranhos retidos" (ou *retained foreign bodies*). A sala de operações possui um dos mais complexos ambientes de trabalho que se pode encontrar nos cuidados de saúde. Esta complexidade manifesta-se a nível dos protocolos, dos tratamentos, da evolução da tecnologia, da necessidade de lidar rapidamente com mudanças de condições drásticas, stress, etc.. Assim, os corpos estranhos retidos são derivados de um ambiente stressante e complexo, mas o risco aumenta com as seguintes variáveis:

- Operações de longa duração, que aumentam o cansaço da equipa médica;
- Mudanças de equipas no decorrer das cirurgias, o que pode causar perda de informação;
- Pacientes obesos;

- Urgências, sendo que a contagem dos instrumentos cirúrgicos passa a ser uma prioridade menor quando a vida do paciente está em perigo;
- Mudanças inesperadas nos procedimentos, o que aumenta o stress e, muitas vezes, provoca a introdução de mais utensílios do que o inicialmente previsto;
- Dualidade das tarefas pelas enfermeiras que são responsáveis pela contagem, o que as pode distrair de tarefas mais importantes;
- Má contagem.

A retenção de objectos estranhos durante as cirurgias pode causar os mais variados efeitos biológicos, que se manifestam através dos sintomas mais comuns: dores, irritações, massa palpável, obstruções, febre, náuseas e perda de peso. Em alguns casos, podem ocorrer complicações tais como: calcificações, a adesão com tecido circundante, ou o aparecimento de abcessos. Estas situações podem levar a uma infecção generalizada e até mesmo à morte do paciente. Estas condições podem também trazer consequências financeiras. Pois, na descoberta de um objecto estranho, o paciente vai ser novamente submetido a uma cirurgia para que se proceda à sua remoção. Esta situação só por si já envolve despesas adicionais, sendo que existem também casos em que os pacientes apresentam queixa, o que acarreta custos suplementares com tribunais e/ou indemnizações. Contudo, para que se possa aplicar um sistema RFID no reconhecimento e rastreamento de instrumentos cirúrgicos devem existir etiquetas resistentes a altas temperaturas (esterilização), resistentes quando submetidas a pressões elevadas, impermeáveis à água, e tolerantes a ondas ultra-sónicas devido à lavagem dos instrumentos, devem permitir a protecção dos dados contidos nas etiquetas e por fim, ter as dimensões necessárias para que possam ser colocadas nos instrumentos cirúrgicos [85].

4.1.6. Etiqueta RFID implantável no corpo humano

Como já aqui foi referido por diversas vezes, a evolução da tecnologia permitiu potencializar a identificação por radiofrequência. Uma das aplicações é de utilizar as etiquetas na medição de sinais biológicos e processos fisiológicos. Este procedimento só é possível partindo da evidência que cada processo biológico leva a modificações das propriedades eléctricas dos tecidos. Assim, quando inserida no meio de células, a etiqueta vai recolher os sinais eléctricos produzidos por elas. Através de uma variação de impedância e do ganho da sua antena as etiquetas detectam automaticamente uma mudança da variável estudada. Esta variação é comunicada ao leitor através de modulação análoga da energia por retro-espalhamento ou através de codificação digital, isto no caso de as etiquetas possuírem *microchips*.

Para que um sistema com esta finalidade seja viável é necessário que a etiqueta a implantar observe certos requisitos. O primeiro é ter dimensões reduzidas, assim, desde logo os dispositivos activos só dificilmente poderão ser utilizados, visto que as baterias exigiriam um espaço considerável. É também importante que a etiqueta seja feita ou envolvida por materiais bio-compatíveis, minimizando assim os riscos de reacções adversas por parte do corpo humano, tais como infecções ou rejeição do implante. Como é evidente, e pelas razões já referidas no capítulo anterior, é essencial que o sistema respeite as normas IEC/EN 60601. O último requisito a observar prende-se com o controlo electrónico remoto da variável [86].

Assim, nessas aplicações, a antena é um elemento decisivo, pois tem que responder a determinadas necessidades energéticas e biológicas para que o sistema possa funcionar sem prejudicar o meio em que está inserido: as células humanas. Para ser eficiente, a antena deverá, tal como a etiqueta, ser de dimensões reduzidas, bio-compátivel e o menos invasiva possível. Para além destas características, e por ser implantada no corpo humano, é necessário ter em consideração o local e a anatomia do espaço onde é colocada a antena. Por exemplo, a antena poderá apresentar-se na forma de um vaso (sanguíneo ou linfático), ser implantada numa prótese cirúrgica ou ortopédica [87].

No entanto, é importante ter em atenção que o corpo humano pode atenuar as radiações electromagnéticas, prejudicando assim o desempenho das comunicações.

4.2. Melhoria da eficiência operacional

4.2.1. Optimização da gestão dos instrumentos médicos

Os hospitais possuem uma numerosa quantidade de equipamentos, na sua grande parte dispendiosos. No entanto, todos os anos são gastos recursos excessivos (monetários e de produtividade), com equipamentos deslocados, roubados ou perdidos. Monetários na medida em que, a maior parte do equipamento terá que ser reposta ou alugada a outra entidade. Em relação à produtividade, estudos feitos comprovam que as enfermeiras desperdiçam demasiado tempo a procurar equipamentos médicos, desviando-as assim de cuidar dos seus pacientes [55].

A identificação por radiofrequência é uma solução adequada para esta problemática, pois permite identificar e localizar qualquer objecto (cadeira de rodas, raio-X portátil, bombas de infusão, máquinas de monitorização de pacientes, entre muitos outros) munido de uma etiqueta, mesmo que este esteja em movimento no hospital [55, 88, 89].

Para satisfazer estas necessidades, a Exavera Technologies criou o eShepherd™. Este sistema combina uma rede de banda larga *WI-FI* segura, dispositivos RFID e etiquetas Vera-

T™. No caso do rastreamento de equipamentos médico são colocadas etiquetas activas, operando numa frequência de 868 MHz ou 2,4 GHz (para a Europa), que têm um alcance de leitura de aproximadamente 27 metros. Para facilitar a transmissão e actualização de dados em tempo real, o eShephard™ utiliza também routers e está ligado ao SIH (Sistema de Informação Hospitalar) [90].

Com este sistema, o pessoal de saúde pode consultar, em qualquer momento, a localização dos equipamentos disponíveis, assim como, realizar a qualquer momento um inventário de todo o equipamento médico do hospital. Sendo que estas operações podem ser efectuadas com o auxílio de um simples computador, PDA ou tablete. No caso de alguém tentar sair do hospital indevidamente com algum aparelho, um alarme será activado. Para ser assegurada uma comunicação segura entre as diversas componente do eShephard™ e também com o SIH, são utilizadas *firewalls* internas e técnicas de encriptação [91].

4.2.2. Análise dos dados operacionais e logística

A implementação e recolha de dados realizada pelos sistemas RFID podem contribuir para um melhor aproveitamento dos recursos (custos/tempo). Os dados recolhidos podem ser utilizados na realização de estudos que auxiliem na definição de procedimentos para aumentar a produtividade e evitar desperdícios [92].

4.3. Acelerar o tratamento médico

A MedicAlert Foundation, uma organização sem fins lucrativos de informática em cuidados de saúde, criou o MedicAlert. Este sistema consiste em embutir uma etiqueta em jóias ou num cartão que se possa transportar na carteira. Estas etiquetas contêm informações variadas, tais como: a identificação da pessoa, o seu registo médico e outras informações pertinentes acerca da sua saúde (medicação, alergias, e as pessoas a contactar em caso de emergência). Porém, é importante salientar que é o cliente quem decide quais as informações a constar no registo. Este sistema foi concebido com o intuito de facilitar e acelerar o tratamento médico. Isto acontece na medida em que, permite à equipa médica de um hospital aceder aos dados de um pessoa que dê entrada numa situação de emergência. A equipa médica pode aceder de imediato a toda informação clínica pertinente do paciente, facilitando o diagnóstico e ajudando no tratamento. A equipa médica pode ter acesso imediato a dados como: o tipo sanguíneo, as alergias do doente, ou as doenças existentes. O MedicAlert torna-se também muito importante para pessoas que sofrem de doenças que afectam a memória (como por exemplo, Alzheimer). Também as pessoas portadoras de doenças que possam causar perda de consciência, tais como diabetes ou epilepsia, podem

retirar partido desta tecnologia. Pois, aquando da chegada do doente ao hospital, este poderá estar inconscientes ou com dificuldades em comunicar. Nestes casos, acedendo às informações contidas na etiqueta, o pessoal de saúde poderá aceder às informações que poderão salvar a vida do paciente ou pelo menos facilitar e acelerar o seu tratamento [93, 94].

Além disso, em todos os cartões e jóias consta o número de telefone para o qual a equipa médica pode ligar. Com base no número de série da etiqueta é possível obter informações adicionais acerca do paciente. A assistência está disponível 24 horas por dia, 7 dias por semana. A etiqueta utilizada nesta aplicação é passiva, opera à frequência de 13,56 MHz e observa a norma ISO 15693 (ver anexo A). Esta aplicação tem causado muita controvérsia em relação à privacidade dos utilizadores, pois, foi desenvolvida para utilização em caso de emergência médica. O problema advém do facto de os dados residentes na etiqueta poderem ser facilmente acedidos, já que a sua encriptação e codificação são bastante vulneráveis [93].

5. Sistemas RFID e suas implicações na saúde e instalações médicas

Neste capítulo iremos discutir os efeitos dos campos electromagnéticos gerados pelos sistemas RFID em pessoas e equipamentos.

5.1. Efeito do campo electromagnético sobre o corpo humano

A identificação por radiofrequência é um sistema em crescimento onde a investigação e inovação são uma constante. O conhecimento das possíveis implicações do campo electromagnético ou electromagnetic interference (EMI), princípio base desta tecnologia, sobre a saúde humana é ainda muito escasso [67].

O tecido humano contém na sua composição principal, moléculas de água, as quais têm tendência para absorver a energia contida nas ondas de radiofrequência. A taxa de absorção específica (Specific Absorption Rate- SAR) é a medida dosimétrica que mede a taxa de energia de radiofrequência absorvida pelos tecidos humanos quando expostos a um campo electromagnético. No trabalho [95], os autores analisaram a SAR absorvida pela cabeça humana e ombros, quando expostos a um campo electromagnético gerado por um leitor de RFID de UHF, que funciona segundo as normas da Comissão Federal de comunicação ou FCC. Os testes foram efectuados para potências de saída de 1 W, 10 W e 100 W, com distâncias de 10 e 100 cm entre a antena do leitor e a cabeça da pessoa. É importante salientar que a antena do leitor é um PATCH rectangular com ganho de 7,4 dB. Após efectuar todos os testes e tratar os resultados, observaram que para a distância de 10 cm e 2 leitores existe um intervalo em que o nível de SAR ultrapassa os 1,6 W/kg recomendados pelo FCC, ultrapassando os 2 W/kg [95].

5.2. Interferências do campo electromagnético sobre os outros equipamentos médicos

Uma das dificuldades que advém da implementação de novas tecnologias, especialmente as baseadas em tecnologias *wireless*, na saúde, é o facto de existir a possibilidade de interferência electromagnética com outros equipamentos eléctricos, neste caso equipamentos médicos, alguns essenciais para o suporte de vida [96].

Estas interferências podem surgir de qualquer corrente eléctrica alternada. Na maior parte dos casos, as interferências electromagnéticas são imprevisíveis podendo variar de

aparelho para aparelho. Assim, é importante a existência de uma classificação para especificar os tipos de incidentes que podem ocorrer devido a essa interferência. Estes podem ser divididos em 3 grupos, consoante os danos causados: ligeiros, significantes e perigosos. Os incidentes ligeiros influenciam a monitorização do paciente, não existindo contudo a necessidade de cuidados extras. Incidentes significativos influenciam a monitorização, causando medições imprecisas que geram falsos alarmes ou, pelo contrário, a falta deles, acarretando assim a necessidade de uma atenção particular. Os incidentes perigosos provocam mudanças inesperadas nas funções do equipamento com efeitos directos no paciente. Neste grupo encontram-se situações que vão desde a alteração de parâmetros configurados previamente até ao desligar do equipamento. É contudo importante salientar que quase todos (para não dizeres todos) os testes são efectuados com simuladores, isto é, máquinas que simulam sinais biológicos humanos [96], [97].

Não são muitos os estudos que se debruçam sobre esta problemática e as opiniões dos existentes são divergentes. Assim vejamos. No estudo [97] realizado em 2008, os autores efectuaram testes em 41 equipamentos médicos, sendo que, cada equipamento sofre três testes: um por cada plano (sagital, frontal e transversal). Para estes testes, foram utilizados dois tipos de sistemas RFID: um passivo, cujo leitor opera a uma frequência de 868 MHz e potência varia entre os 2 e 4 Watts; e um activo, cujo leitor opera a uma frequência de 125 kHz. Para efectuar os testes, foi seguido o protocolo ANSI C 63.18.1997.

Este protocolo foi especificamente pensado para avaliar a susceptibilidade de dispositivos médicos a interferências electromagnéticas. Também permite determinar a distância mínima, entre o equipamento médico e o leitor, a que as interferências não ocorram. As variáveis envolvidas neste teste incluem a distância entre o leitor RFID e o equipamento, a potência que advém da fonte, e a posição relativa entre o leitor RFID e o equipamento testado [98].

Na figura 31 encontra-se um fluxograma representativo dos procedimentos efectuados no teste dos equipamentos médicos.

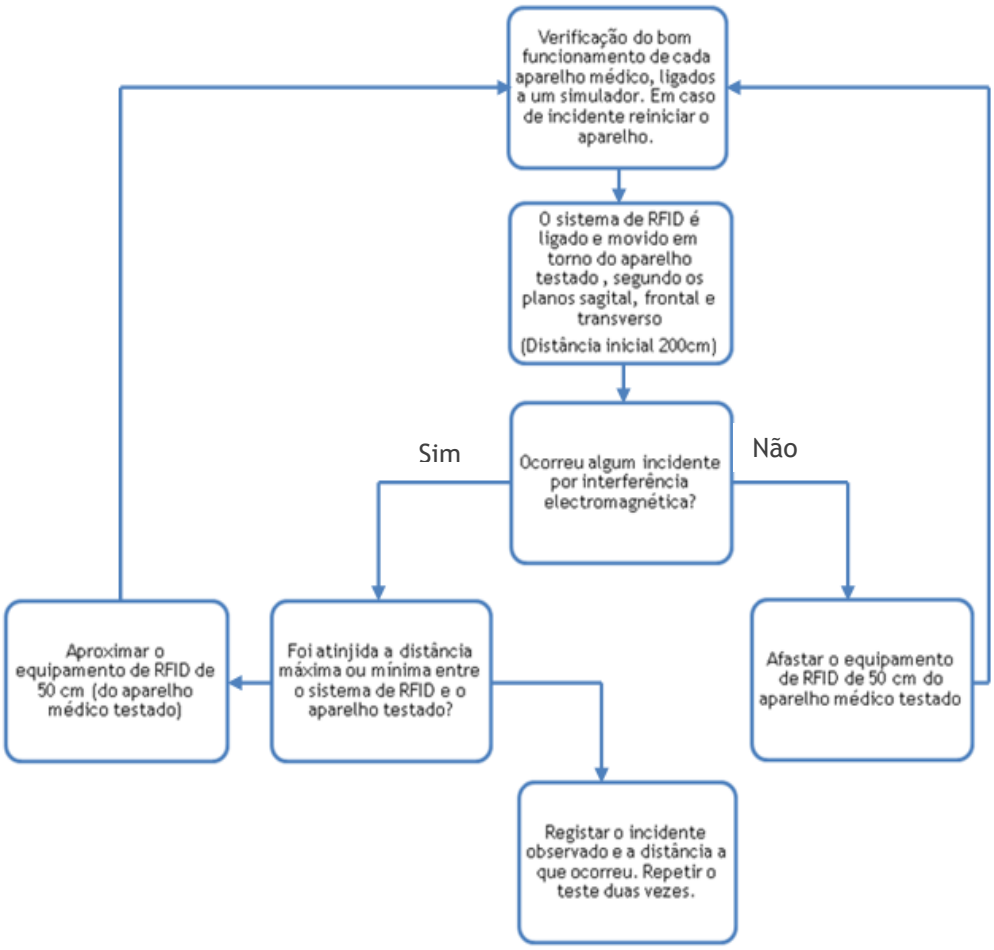


Figura 31: Fluxograma representativo do procedimento do teste [97].

Após efectuar os 123 testes e recolher os resultados foram registados 34 incidentes que tiveram como causa as interferências electromagnéticas, sendo 10 ligeiros, 2 significativos e 22 perigosos. É também importante salientar que, o sistema do tipo activo induziu 26 incidentes contra 8 incidentes para o sistema passivo. A distância média entre o leitor e os diferentes equipamentos médicos nos testes onde ocorreram incidentes electromagnéticos é de 30 cm [97].

No trabalho [99], realizado em 2010, é-nos apresentado um protocolo que tem como finalidade testar e verificar os efeitos de interferências electromagnéticas entre leitores de RFID e bombas de infusão. Este artigo vai mais longe do que o abordado anteriormente. Pois, os autores defendem que é importante a caracterização da distribuição do campo electromagnético vindo do leitor, com o intuito de melhor entender as variações de susceptibilidade entre equipamentos similares. Assim, foi utilizado um sistema de medição cilíndrico para avaliar a força do campo magnético nos vários testes. Os testes foram efectuados com 3 bombas de infusão e dois tipos de sistemas RFID: um primeiro que opera na

banda dos 125 kHz e outro na banda dos 13,56 MHz. Na figura 32 encontra-se um fluxograma representativo do procedimento do teste. Contrariamente ao estudo referido anteriormente, não foram observados incidentes decorrentes das interferências electromagnéticas nos testes efectuados.

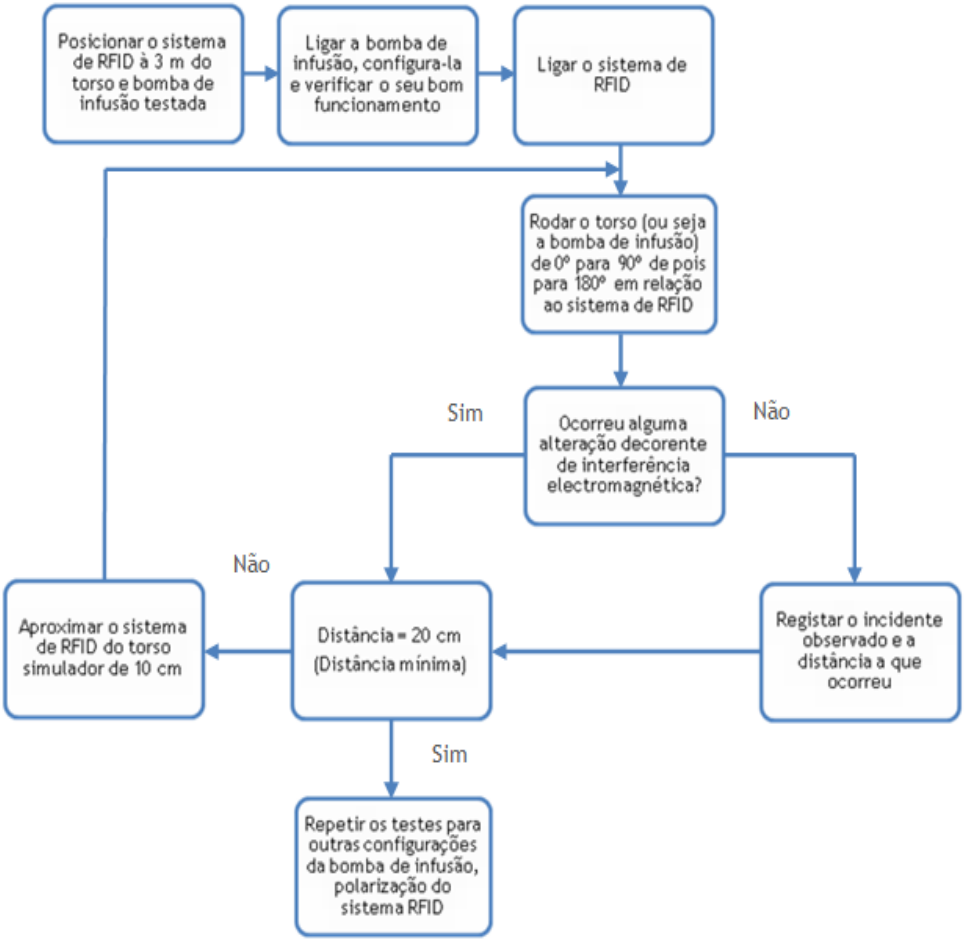


Figura 32: Fluxograma representativo do procedimento do teste [99].

No entanto, importa salientar que estes testes não seguiram o protocolo ANSI C 63.18.1997 (como os restantes trabalhos abordados) e comporta diferenças significativas tais como os planos. No ANSI C 63.18.1997 os testes são realizados segundo três planos, enquanto que neste trabalho são explorados unicamente as vertentes horizontais e verticais. Uma possível causa encontrada pelos autores pela ausência de interferências electromagnética é o facto de as bombas de infusão serem de tamanho reduzido, sendo que, a tensão induzida nas partes condutoras da bomba de infusão, quando expostas aos leitores de RFID, é menor do que 0,5V.

O artigo [96], realizado já em 2011, foram testados 32 equipamentos médicos de diversos tipos com um sistema RFID de baixa frequência RuBee™ (131 kHz) que segue o

protocolo IEEE 1902.1. A inovação neste teste é que foram adicionadas antenas externas ao sistema RFID, mais precisamente ao leitor. Os testes foram efectuados com dois tipos de antenas: ranger e RPM (*Rotating Phase Multiplexed*). Estas antenas foram adicionadas para verificar se se observavam alterações nas interferências electromagnéticas baseadas na orientação das antenas. Como no trabalho anterior, foi medida a força do campo electromagnético em todos os testes. Os testes seguiram o procedimento enunciado na norma ANSI C 63.18 (tal como o primeiro trabalho referido). No fim dos testes foram contabilizados 14 incidentes (7 ligeiros, 5 significativos e 2 perigosos) em 8 aparelhos médicos diferentes. Com as medições efectuadas puderam observar que não houve alterações significativas na força do campo electromagnético com o aumento ou diminuição da distância entre a antena e os aparelhos médicos, ou com a ocorrência ou não de incidentes electromagnéticos. Confirmou-se também que a orientação das antenas não teve qualquer influência do campo electromagnético nas interferências electromagnéticas.

Nos diversos trabalhos publicados, verificou-se que um dos parâmetros que mais influencia as interferências electromagnéticas, entre sistemas RFID e equipamentos médicos, é a distância entre os sistemas e a tensão de saída do leitor de identificação por radiofrequência. Por sua vez, a tensão de saída depende directamente da frequência de funcionamento do sistema. Assim, a imunidade electromagnética é um requisito essencial nos equipamentos médicos. O IEC 60601 (para os Estados Unidos da América) e o EN 60601 (para a Europa) são dois protocolos praticamente idênticos que especificam as normas técnicas para segurança (IEC/EN 60601-1) e a compatibilidade electromagnética (IEC/EN 60601-1-2). Sendo que, nesta última, estão especificadas os requerimentos e procedimentos para testar a imunidade e compatibilidade electromagnética. Este protocolo fornece fórmulas que permitem calcular a distância mínima recomendada, entre um equipamento e um sistema RFID, dado o nível de imunidade dos equipamentos médicos e a taxa de potência máxima de saída do leitor de RFID [86].

Na tabela 14 estão representadas as frequências de funcionamento e respectivas fórmulas para o cálculo da distância mínima entre um equipamento médico e um sistema RFID.

Tabela 14: Frequências de funcionamento e respectiva fórmula para calcular a distância mínima recomendada entre um equipamento médico e sistema RFID, onde D representa a distância em [m], P é a taxa de potência máxima de saída do sistema RFID em [W], V é o nível de imunidade do equipamento médico em [V] e E representa o nível de imunidade dos equipamentos médicos em [V/m] [86].

Frequência de funcionamento	**150 kHz – 80 MHz**	**80 MHz – 800 MHz**	**800 MHz – 2,5 GHz**
Fórmula para calcular a distância mínima recomendada	$D = 12\sqrt{P/V}$	$D = 12\sqrt{P/E}$	$D = 23\sqrt{P/E}$

5.3. Métodos para solucionar as interferências

Como foi visto nos subcapítulos anteriores, a identificação por radiofrequência oferece muitas vantagens por ser uma tecnologia *wireless*. Contudo, estas mesmas vantagens podem levar a problemas relacionados com interferências electromagnéticas, de dois tipos. O primeiro depara-se com o facto de sistemas RFID poderem interferir com o normal funcionamento de equipamentos médicos, alguns dos quais essenciais para o suporte de vida, podendo assim por em risco a segurança dos pacientes. Por outro lado, os equipamentos médicos também podem gerar campos electromagnéticos radiados que podem afectar o normal desempenho dos sistemas RFID [100].

Desta feita, é muito importante encontrar soluções que vão de encontro à resolução desta problemática, para que os sistemas RFID sejam implementados de forma eficiente e segura. Nesse sentido, foi criada uma área denominada de "compatibilidade electromagnética" ou *electromagnetic compatibility* - EMC, que segunda a comissão europeia, representa toda e qualquer técnica ou tecnologia que reduza as interferências e aumenta a imunidade dos equipamentos [101]. Assim, já existem algumas normas específicas para testar e evitar as interferências electromagnéticas e levar a uma crescente compatibilidade electromagnética, tais como o ANSI C 63.18.1997, abordado anteriormente.

Seguindo esta abordagem, existem várias empresas, tais como a Intertek ou a MET, especializadas em testar e certificar a conformidade dos equipamentos em relação às EMI/EMC, incluindo o ambiente em que estes estão inseridos [102], [103]. Na Europa essa certificação tem que estar de acordo com a directiva 2004/108/EC [101] e os testes podem ser efectuados segundo o protocolo ETSI EN 301 489-1 V1.4.1 (2002-08) [104].

Uma abordagem mais prática para resolver esta problemática é proposta por empresas que criaram produtos que atenuam, conduzem ou protegem os equipamentos das EMI. Por exemplo, podemos encontrar a COMPELMA que criou atenuadores de RF, ferrites

supressoras de EMI e indutores. Estes últimos têm como função proteger os circuitos de altas frequências, actuando como filtros passa-baixo. Os atenuadores de RF (ver figura 33) são constituídos por ferrites que podem ser disponibilizados em várias formas e espessuras, direccionados para uma variada gama de frequências. Sendo que, estes apresentam uma permeabilidade inicial de 7μ iac, uma resistência eléctrica de 10^{12} Ω.cm, e uma tensão de ruptura de dieléctrico de 9 kV, para uma espessura de 1 mm [105].

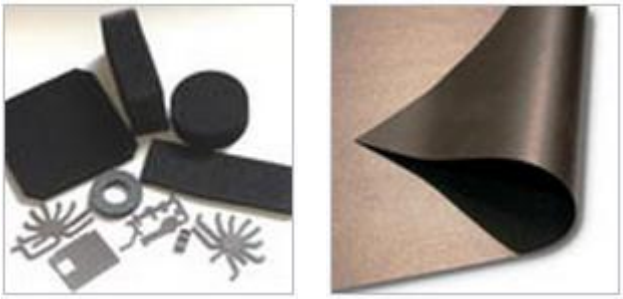


Figura 33: Atenuadores de RF da COMPELMA [106].

Em relação às ferrites de supressão de EMI, estas são constituídas na sua grande parte por uma liga de Níquel-Zinco com revestimento variado, e são bastante eficientes no caso de altas frequências [107].

Outra empresa, a MTC, comercializa janelas "escudos" contra interferências eléctricas. Estas são constituídas por um revestimento de "Indium Tin Oxide" e podem ter uma resistência de superfície que pode variar dos 2,5 aos 2500 Ω.cm. Sendo que a base da janela pode ser de vidro ou plástico, esta é unida ao revestimento através de prata de barramento [108].

Em conclusão deste subcapítulo, foi visto que existe legislação e protocolos em relação à problemática das EMI e EMC, contudo as normas empregues variam de fabricante para fabricante. Assim, é necessário desenvolver normas uniformizadas que possam permitir uma utilização segura e universal, principalmente em meio hospitalar.

6. Perspectivas futuras e conclusão

6.1. Conclusão

Esta dissertação teve como objectivo principal estudar a aplicabilidade da identificação por radiofrequência em meio hospitalar. Começou-se por descrever os princípios físicos que regem esta tecnologia. De seguida, realizou-se um estudo sobre o funcionamento dos diferentes tipos de sistemas RFID, dos seus elementos e interacção entre eles. De acordo com o capítulo 3, testou-se a utilização do módulo TRF760EVM, da Texas Instrument, de forma a promover uma autêntica interacção com um sistema real de identificação por radiofrequência. Na etapa final do trabalho, enfatizou-se a importância da utilização e empregabilidade de um sistema RFID em meio hospitalar. Foi também abordada a temática da possível interferência de sistemas desta natureza com os demais equipamentos existentes num meio hospitalar.

No final deste trabalho pôde-se retirar as seguintes ilações. A primeira depreende-se com o facto de a tecnologia RFID ser relativamente recente, apresentando um grande potencial de aplicabilidade em novas áreas de mercado. Um exemplo de sucesso, é a sua aplicação nas áreas de gestão de cadeias de transporte logístico. É também considerada por muitos, como a tecnologia que irá substituir a tecnologia dos códigos de barra.

Para além dos benefícios da tecnologia em si referenciados, em relação à área da saúde propriamente dita, mais precisamente em ambiente hospitalar, foi demonstrado que a implementação da RFID introduz grandes benefícios em diversas vertentes, tais como:

- Um aumento significativo na segurança dos pacientes e prevenção de erros médicos pela identificação e rastreamento dos pacientes, gestão segura da farmácia e das amostras de laboratório;
- Uma melhoria nítida da eficiência operacional que passa pela optimização da gestão dos equipamentos e recursos médicos e pela análise dos dados operacionais, permitindo a introdução de estratégias para aumentar a eficiência e baixar os custos;
- Por fim, optimizar o tratamento médico pelo fácil acesso aos dados essenciais relativo ao paciente.

Vários estudos demonstraram que podem realmente ocorrer interferências electromagnéticas nos equipamentos médicos provocadas pelo funcionamento de sistema RFID. Contudo, existem várias empresas no mercado que, para prevenir eventuais EMI, realizam testes no local de implementação e para verificar eventuais incompatibilidades, segundo protocolos criados para esses efeitos. As EMI também podem ser evitadas através de

dispositivos tais como indutores (responsáveis pela atenuação de altas frequências), atenuadores de RF e ferrites de supressão que também são utilizadas na confeição de escudos EMI.

No meu entender, é necessário um estudo mais rigoroso sobre as EMI/EMC e efeitos do acampo electromagnético sobre o corpo humano, para uma implementação controlada e segura. São também necessários progressos e desenvolvimento a nível da tecnologia e de custos (ver subcapítulo seguinte) para que a RFID seja amplamente aceite e implementada.

6.2. Perspectivas futuras

A identificação por radiofrequência é uma tecnologia emergente que já conquistou o mercado do retalho. Mas outros mercados apresentam grande interesse por esta tecnologia, nomeadamente o da saúde, onde decorrem estudos que procuram formas de retirar o melhor partido desta tecnologia. Algumas implementações existentes permitem já concluir que se trata de uma área de aplicação com grande potencial. No entanto, para que esta tecnologia seja aceite e aplicada com sucesso em ambientes médicos é necessário que mais progressos científicos e tecnológicos sejam alcançados em diversas áreas.

O factor que mais tem contribuído para atrasar a aplicação em grande escala dos sistemas RFID prende-se com o custo de fabrico e de implementação. Para além de se ter que adquirir as etiquetas e os leitores, cujos preços variam consoante os requisitos e aplicabilidade desejadas, é também necessário estabelecer um plano de incorporação. Não só deve ser realizada uma adaptação do sistema ao ambiente em que este irá ser utilizado, mas também como será importante dotar os profissionais das competências necessárias para operar de forma correcta estes dispositivos.

A grande diversidade de normas e protocolos pode provocar na indústria uma sensação de frustração. Embora estejam a ser desenvolvidos leitores que funcionam com múltiplos protocolos, a uniformização de normas e protocolos traria mais benefícios. Em concreto, iria garantir a compatibilidade entre equipamentos de fabricantes diferentes. Uma consequência directa desta medida seria o aumento da procura e consequente diminuição do custo de aquisição.

Actualmente, estudos são realizados no sentido de melhorar diversos aspectos a nível tecnológico. Exemplo disso é a optimização da eficácia da transmissão de dados entre a antena da etiqueta e a antena do leitor, uma vez que a posição relativa entre as duas antenas influencia a comunicação entre os dois elementos. Uma possível solução para resolver este problema seria dotar o leitor com várias antenas apresentando orientações diferentes. Outra problemática em estudo diz respeito ao facto de alguns materiais degradarem a qualidade das transmissões, impedindo assim uma comunicação eficiente. Assim, como com quaisquer

outros equipamentos tecnológicos é importante investir mais em pesquisas e desenvolvimento, para se conseguir fazer equipamentos de menores dimensões mas que sejam mais eficientes e que possam incorporar maiores funcionalidades a preços mais competitivos.

Por fim, mas não menos importante, é a aceitação social desta tecnologia, sendo que existe uma preocupação cada vez maior em relação à segurança dos dados contidos nas etiquetas e à privacidade pessoal. Em relação à segurança, e como já foi referido no capítulo correspondente, existem sistemas de defesa nas etiquetas mais evoluídas, contudo, as mais baratas são desprovidas dessas características. Há, portanto, uma necessidade de que estas implementações consigam introduzir essa segurança, sem acréscimo considerável de custo, na medida em que é destas (as de menor custo) que se espera serem as impulsionadoras da tecnologia RFID.

Em relação à privacidade e no caso concreto dos hospitais, existe algum desconforto por parte dos profissionais de saúde, que têm receio que ao transportarem uma etiqueta de RFID (para serem localizados de maneira rápida quando necessário), esta seja também utilizada como método de vigilância. Alguns dos inqueridos também expressaram a preocupação de que esta tecnologia lhes venha a dar mais afazeres. Assim, como foi referido, é necessário formar os profissionais para que estes possam entender a finalidade das aplicações e os métodos de funcionamento.

Bibliografia

[1] J. J. Roh, *et al.*, "Classification of RFID adoption: An expected benefits approach," *Information & Management,* vol. 46, pp. 357-363, 2009.

[2] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, (2^{cnd} Edition)*: John Wiley & Sons, Ltd, 2003.

[3] C. Yang, *et al.*, "Identification of barcode beacon and its application in underground mining," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, 2010, pp. V1-128-V1-132.

[4] R. Muniz, *et al.*, "A robust software barcode reader using the Hough transform," in *Information Intelligence and Systems, 1999. Proceedings. 1999 International Conference on*, 1999, pp. 313-319.

[5] A. D. Yalcinkaya, *et al.*, "Polymer magnetic scanners for bar code applications," *Sensors and Actuators A: Physical,* vol. 135, pp. 236-243, 2007.

[6] K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and identification.*, Second Edition ed.: John Wiley & Sons, Ltd., 2003.

[7] H. Tan, "The Application of RFID Technology in the Warehouse Management Information System," presented at the Electronic Commerce and Security, 2008 International Symposium on, 2008.

[8] J. S. I. Patrick, *RFID For Dummies*: John Wiley & Sons, Inc., 2007.

[9] R. Weinstein, "RFID: a technical overview and its application to the enterprise," *IT Professional,* vol. 7, pp. 27-33, 2005.

[10] N. C. Wu, *et al.*, "Challenges to global RFID adoption," *Technovation,* vol. 26, pp. 1317-1323, 2006.

[11] A. Wui, *et al.*, "Critical Issues that Will Determine the Future of RFID," in *Management of Mobile Business, 2007. ICMB 2007. International Conference on the*, 2007, pp. 48-48.

[12] C. M. Roberts, "Radio frequency identification (RFID)," *Computers & Security,* vol. 25, pp. 18-26, 2006.

[13] H. Stockman, "Communication by Means of Reflected Power," *Proceedings of the IRE,* vol. 36, pp. 1196-1204, 1948.

[14] J. Landt, "The history of RFID," *Potentials, IEEE* vol. 24 Issue:4, pp. 8 - 11, 2005.

[15] R. Bunduchi, *et al.*, "Mapping the benefits and costs associated with process innovation: The case of RFID adoption," *Technovation,* vol. 31, pp. 505-521, 2011.

[16] M. S. Philipose, J.R.; Jiang, B.; Mamishev, A.; Sumit Roy; Sundara-Rajan, K., "Battery-free wireless identification and sensing," *Pervasive Computing, IEEE,* vol. 4, pp. 37- 45, 2005.

[17] R. F. Bhattacharyya, C.; Sarma, S., "Low-Cost, Ubiquitous RFID-Tag-Antenna-Based Sensing," *Proceedings of the IEEE* vol. 98, pp. 1593- 1600 2010.

[18] A. R. Sani, M.; Foster, R.; Yang Hao, "Antennas and Propagation of Implanted RFIDs for Pervasive Healthcare Applications," *Proceedings of the IEEE* vol. 98, pp. 1648- 1655 2010.

[19] R. R. Gadh, G.; Michael, K.; Huang, G.Q.; Prabhu, B.S.; Chu, P, "RFID—A Unique Radio Innovation for the 21st Century," *Proceedings of the IEEE* vol. 98, pp. 1546- 1549, 2010.

[20] E. W. T. Ngai, *et al.*, "RFID research: An academic literature review (1995-2005) and future research directions," *International Journal of Production Economics,* vol. 112, pp. 510-520, 2008.

[21] K. Domdouzis, *et al.*, "Radio-Frequency Identification (RFID) applications: A brief introduction," *Advanced Engineering Informatics,* vol. 21, pp. 350-355, 2007.

[22] A. Sarac, *et al.*, "A literature review on the impact of RFID technologies on supply chain management," *International Journal of Production Economics,* vol. 128, pp. 77-95, 2010.

[23] W. M. G. Wismans, "Identification and registration of animals in the European Union," *Computer and electronics in agriculture,* vol. 24, pp. 99- 108, 1999.

[24] S. Streit, *et al.*, "Automatic life-long monitoring of individual insect behaviour now possible," *Urban & Fischer Zoology,* vol. 106, pp. 169-171, 2003.

[25] K. Coyle, "Management of RFID in Libraries," *The Journal of Academic Librarianship,* vol. 31, pp. 486- 489, 2005.

[26] P. Sanghera and F. Thornton, "Chapter 2 - The Physics of RFID," in *How to Cheat at Deploying and Securing RFID*, ed Burlington: Syngress, 2007, pp. 23-50.

[27] D. K. Klair, *et al.*, "A Survey and Tutorial of RFID Anti-Collision Protocols," *Communications Surveys & Tutorials, IEEE,* vol. 12, pp. 400-421, 2010.

[28] P. V. Nikitin and K. V. S. Rao, "Theory and measurement of backscattering from RFID tags," *Antennas and Propagation Magazine, IEEE,* vol. 48, pp. 212-218, 2006.

[29] M. Ward and R. v. Kranenburg, "RFID: Frequency, standards, adoption and innovation," *JISC Technology and Standards Watch,* May 2006.

[30] (2005, 10/09/2011). *A Summary of RFID Standards*. Available: http://www.rfidjournal.com/article/view/1335

[31] EPCglobal. (2007). *Electronic Product Code (EPC): An Overview*. Available: http://www.gs1.org/docs/epcglobal/an_overview_of_EPC.pdf

[32] D. Taggart and E. Burger, "The State of RFID Implementation and Its Policy Implications: An IEEE-USA White Paper," *IEEE,* April 2009.

[33] (2011, 03/07/2011). *ISO RFID Standards: A Complete List*. Available: http://rfid.net/basics/186-iso-rfid-standards-a-complete-list-

[34] V. Najafi, *et al.*, "A dual mode UHF EPC Gen 2 RFID tag in 0.18 µm CMOS," *Microelectronics Journal,* vol. 41, pp. 458-464, 2010.

[35] S. Preradovic, *et al.*, "RFID Transponders," *IEEE microwave magazine,* vol. 9, October 2008.

[36] J. Heidrich, *et al.*, "The Roots, Rules, and Rise of RFID," *Microwave Magazine, IEEE,* vol. 11, pp. 78-86, 2010.

[37] C. Zhi Ning and Q. Xianming, "Antennas for RFID applications," in *Antenna Technology (iWAT), 2010 International Workshop on*, 2010, pp. 1-4.

[38] Y.-W. Ma, *et al.*, "Load-balancing mechanism for the RFID middleware applications over grid networking," *Journal of Network and Computer Applications,* vol. 34, pp. 811-820, 2011.

[39] B. Chowdhury and R. Khosla, "RFID-based Hospital Real-time Patient Management System," in *Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS International Conference on*, 2007, pp. 363-368.

[40] H. Knospe and H. Pohl, "RFID security," *Information Security Technical Report,* vol. 9, pp. 39-50, 2004.

[41] A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on,* vol. 24, pp. 381-394, 2006.

[42] J. Ayoade, "Roadmap to solving security and privacy concerns in RFID systems," *Computer Law & Security Review,* vol. 23, pp. 555-561, 2007.

[43] J. C. H.-C. Pedro Peris-Lopez, Juan M. Estevez-Tapiador, Arturo Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions," *Personal Wireless Communications (PCW),* vol. 4217, pp. 159-170, Sepetember 2006 2006.

[44] M. F. Mubarak, *et al.*, "A critical review on RFID system towards security, trust, and privacy (STP)," in *Signal Processing and its Applications (CSPA), 2011 IEEE 7th International Colloquium on*, 2011, pp. 39-44.

[45] Z.-h. Ding, *et al.*, "A taxonomy model of RFID security threats," in *Communication Technology, 2008. ICCT 2008. 11th IEEE International Conference on*, 2008, pp. 765-768.

[46] Qinghan Xiao, *et al.*, "RFID Security Issues in Military Supply Chains," *Availability, Reliability and Security, 2007. ARES 2007,* pp. 599 - 605, 2007.

[47] Mike Burmester and B. D. Medeiros, "RFID Security: Attacks, Countermeasures and Challenges," *CiteSeerX - Scientific Literature Digital Library and Search Engine (United States),* 2007.

[48] L. Leinweber, *et al.*, "A minimal protocol with public key cryptography for identification and privacy in RFID tags," in *Signals, Circuits and Systems, 2009. ISSCS 2009. International Symposium on*, 2009, pp. 1-4.

[49] L. Batina, *et al.*, "Public-Key Cryptography for RFID-Tags," in *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops '07. Fifth Annual IEEE International Conference on*, 2007, pp. 217-222.

[50] J.-c. R. Junichiro Saito , Kouichi Sakurai, "Enhancing privacy of universal re-encryption scheme for RFID tags," *Embedded and Ubiquitous Computing – EUC 2004, LNCS 3207,* 2004.

[51] P. Hamalainen, *et al.*, "Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core," in *Digital System Design: Architectures, Methods and Tools, 2006. DSD 2006. 9th EUROMICRO Conference on*, 2006, pp. 577-583.

[52] M. Feldhofer, *et al.*, "Strong Authentication for RFID Systems Using the AES Algorithm

Cryptographic Hardware and Embedded Systems - CHES 2004." vol. 3156, M. Joye and J.-J. Quisquater, Eds., ed: Springer Berlin / Heidelberg, 2004, pp. 85-140.

[53] D.-H. Shih, *et al.*, "Taxonomy and survey of RFID anti-collision protocols," *Computer Communications*, vol. 29, pp. 2150-2166, 2006.

[54] C. Tao and J. Li, "Analysis and Simulation of RFID Anti-collision Algorithms," in *Advanced Communication Technology, The 9th International Conference on*, 2007, pp. 697-701.

[55] X. Qu, *et al.*, "A model for quantifying the value of RFID-enabled equipment tracking in hospitals," *Advanced Engineering Informatics*, vol. 25, pp. 23-31, 2011.

[56] P. Fuhrer and DominiqueGuinard, "Building a Smart Hospital using RFID technologies," presented at the European Conference on eHealth 2006, Fribourg, Switzerland, 2006.

[57] H.-Y. Chien, *et al.*, "Two RFID-based Solutions to Enhance Inpatient Medication Safety," *Journal of Medical Systems*, vol. 35, pp. 369-375, 2011.

[58] G. H. P. Florentino, *et al.*, "Hospital automation system RFID-based: Technology embedded in smart devices (cards, tags and bracelets)," in *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE*, 2008, pp. 1455-1458.

[59] S. Sbrenni, *et al.*, "Use of RFId technology and CCOW standard for patient traceability," in *Software, Telecommunications and Computer Networks (SoftCOM), 2010 International Conference on*, 2010, pp. 17-20.

[60] H. Sheng-Rong, *et al.*, "Intelligent Hospital Space Platform Combined with RFID and Wireless Sensor Network," in *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on*, 2008, pp. 1001-1004.

[61] B. Bacheldor, "RFID Documents Surgery at Huntsville Hospital," *RFID Journal*, 2007.

[62] SkyeTek. (2005, 17/09/2011). *SkyeModule M1*. Available: http://www.skyetek.com/Portals/0/Documents/Products/SkyeModule_M1_DataSheet.pdf

[63] C. t. P. Ltd. (2009, 13/05/2011). *Clarinox WayPoint*. Available: http://www.clarinox.com/docs/Brochures/ClarinoxWayPoint.pdf

[64] C. T. P. Ltd. (2009, 13/05/2011). *ClarinoxWayPoint... asset tracking and active RFID system*. Available: http://www.clarinox.com/index.php?id=37

[65] C. T. P. Ltd. (2009, 13/05/2011). *Clarinox Yulo*. Available: http://www.clarinox.com/docs/Brochures/ClarinoxYuloV3_Small.pdf

[66] B. Chowdhury and R. Khosla, "RFID-based Hospital Real-time Patient Management System," *Computer and Information Science, 2007. ICIS 2007. 6th IEEE/ACIS* pp. 363 - 368 2007.

[67] S. Fiocchi, *et al.*, "Computational exposure assessment of electromagnetic fields generated by an RFID system for mother–newborn identity reconfirmation," *Bioelectromagnetics,* pp. n/a-n/a, 2011.

[68] A. Campos, "Pulseiras electrónicas para recém-nascidos passam a ser obrigatórias nos hospitais," in *Público, acedido em 18/03/2012*, ed, 2008.

[69] R. Tecnologies. (2010, 05/04/2011). *Safe Place*^{R}. Available: http://www.rft.com/RapidCat/WebPageImages/1379/8354//Safe_Place/Infant_Security_Brochure.pdf

[70] LogicPulse. (03/04/2011). *BlueTag*

Solução de segurança para pacientes vulneráveis. Available: http://www.logicpulse.pt/Portals/0/produtos/Folheto_BlueTag_V1_Web.pdf

[71] H. Daud, Yahya, Noorhana, M. Sakri, M Syazwari, "Tagging system for newborn babies RFID sytem (BabyTraXX)," presented at the TK Electrical Engineering Electronics Nuclear Engineering, Malysia, 2010.

[72] B. Bacheldor, "BlueTag Patient-Tracking Comes to North America," *RFID Journal,* 2008.

[73] B. Bacheldor, "St. John's Children's Hospital Deploys RFID to Protect Children," *RFID Journal,* 2009.

[74] J. Dalton, *et al.*, "RFID Technologies in Neonatal Care," 2005.

[75] Ö. E. Çakıcı, *et al.*, "Using RFID for the management of pharmaceutical inventory -- system optimization and shrinkage control," *Decision Support Systems,* vol. In Press, Corrected Proof.

[76] M. Mansor, "Methodological and ethical challenges in investigating the safety of medication administration.," *Nurse Reserchер. ,* vol. 18, pp. 28-32, 2011.

[77] P. Sun, *et al.*, "A New Method to Guard Inpatient Medication Safety by the Implementation of RFID," *Journal of Medical Systems,* vol. 32, pp. 327-332, 2008.

[78] B. Wu, *et al.*, "eWellness: Building a Smart Hospital by Leveraging RFID Networks," in *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, 2005, pp. 3826-3829.

[79] P. Peris-Lopez, *et al.*, "A comprehensive RFID solution to enhance inpatient medication safety," *International Journal of Medical Informatics,* vol. 80, pp. 13-24, 2011.

[80] L. J. Layfield and G. M. Anderson, "Specimen labeling errors in surgical pathology: an 18-month experience.," *American Journal of clinica pathology.,* vol. 134, pp. 466-470, 2010.

[81] J. Collins, "Putting Tags on test Tubes," *RFID Journal,* vol. 922, 2004.

[82] L. Maxell Seiki. (2009, 10/09/2011). *Coil-on-Chip™ Systems*. Available: http://www.maxei.co.jp/products/intelligentmicrotube/eng_index.html

[83] I. Maxell Corporation of America. (2011). *Maxell Coil-On-Chip™ RFID Tag*. Available: http://www.maxell-usa.com/index.aspx?id=4;41;432;0

[84] L. Maxell Seiki. (2009). *Intelligent Microtube Management System*. Available: http://www.maxei.co.jp/products/intelligentmicrotube/eng_index.html

[85] K. Yamashita, *et al.*, "Identification of information surgical instrument by ceramic RFID tag," in *Automation Congress, 2008. WAC 2008. World*, 2008, pp. 1-6.

[86] F. Censi, *et al.*, "RFID in healthcare environment: electromagnetic compatibility regulatory issues," in *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE*, 2010, pp. 352-355.

[87] C. Occhiuzzi and G. Marroco, "Human body sensing: A pervasive approach by implanted RFID tags," presented at the Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on, ROME, 2010.

[88] A. C. Polycarpou, *et al.*, "A healthcare application based on passive UHF RFID technology," in *Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on*, 2011, pp. 2814-2818.

[89] A. Oztekin, *et al.*, "An RFID network design methodology for asset tracking in healthcare," *Decision Support Systems*, vol. 49, pp. 100-109, 2010.

[90] M. Pappu;, *et al.*, "RFiD IN HOSPITALS: ISSUES AND SOLUTIONS," in *Consortium for the Accelereted Deployment of the RFID in distribuition*, 2004.

[91] E. Technologies. (2011, 08/08/2011). *VeraFi™: The heart of a new model in information delivery*. . Available: http://www.exavera.com/healthcare/verafi.php

[92] V. Boginski, *et al.*, "Simulation and Analysis of Hospital Operations and Resource Utilization Using RFID Data," presented at the RFID, 2007. IEEE International Conference on, 2007.

[93] K. R. Foster and J. Jeager, "RFID Inside," *Spectrum, IEEE*, vol. 44, pp. 24 - 29, March 2007.

[94] C. Swedberg, "MedicAlert Aims To RFID-Enable Medical Records," *RFID Journal*, Feb. 2007.

[95] D. D. Arumugam and D. W. Engels, "Impacts of RF radiation on the human body in a passive RFID environment," in *Antennas and Propagation Society International Symposium, 2008. AP-S 2008. IEEE*, 2008, pp. 1-4.

[96] S. Kapa, *et al.*, "Electromagnetic interference of magnetic field based auto identification technologies in healthcare settings," *International Journal of Medical Informatics*, vol. 80, pp. 239-250, 2011.

[97] Remko van der Togt, *et al.*, "Electromagnetic Interference From Radio Frequency Identification Inducing Potentially Hazardous Incidents in Critical Care Medical Equipment," *JAMA The Journal of American Medical Association*, vol. 299, pp. 2884-2890, 2008.

[98] A. P. S. Silva, *et al.*, "Methodology of testing electromagnetic interference caused by active RFId applied with electrocardiography," in *Health Care Exchanges (PAHCE), 2011 Pan American*, 2011, pp. 154-154.

[99] N. J. LaSorte, *et al.*, "In vitro protocol to study the electromagnetic interaction of RFIDs and infusion pumps," in *Electromagnetic Compatibility (APEMC), 2010 Asia-Pacific Symposium on*, 2010, pp. 1084-1087.

[100] M. Fernández Chimeno and F. Silva Martínez, "RFID systems in medical environment: EMC issues," 2012.

[101] C. Europeia. (2004). *Electromagnetic Compatibility (EMC), acedido em 15/10/2012*. Available: http://ec.europa.eu/enterprise/sectors/electrical/emc/

[102] I. G. plc. *EMC Testing, acedido em 15/10/2012*. Available: http://www.intertek.com/emc/

[103] I. MET Laboratories. (2012). *Regulatory RFID Testing, acedido em 15/10/2012*. Available: http://www.metlabs.com/Industries/RFID/Regulatory-RFID-Testing.aspx

[104] E. Organization, "ETSI EN 301 489-1 V1.4.1 (2002-08)," in *Electromagnetic compatibilitymand Radio spectrum Matters (ERM);*

ElectroMagnetic Compatibility (EMC) standard for radio equipment and services;, ed. http://www.etsi.org/deliver/etsi_en/301400_301499/30148901/01.04.01_60/en_30148901v010401p.pdf, 2012.

[105] Compelma, "ABSORBING SHEET - COMAB, acedido em 16/10/2012," 2011.

[106] Compelma. (2011). *RFID ABSORBANTS, acedido em 16/10/2012*. Available: http://www.compelma.com/en/products/rfid-absorbants,29/

[107] Compelma. (2011). *FILTERING - FERRITES, acedido em 16/10/2012*. Available: http://www.compelma.com/medias/pdf/ferrites.pdf

[108] MTC. (2012). *EMC Shielding Products, acedido em 16/10/2012*. Available: http://www.acaltechnology.com/_files/franchise/MTC/Catalogues/MTC_Vents_Windows_100dpi.pdf

Anexo A- Normas

Cartas de identificação:

- ISO 14443 (A e B): carta com circuitos integrados de identificação que não necessita de contacto directo com o leitor - cartas de proximidade;
- ISO 15693: carta com circuitos integrados de identificação que não necessita de contacto directo com o leitor - cartas de vizinhança.

Air interface (frequency) standards:

- ISO18000- 1: Parâmetros genéricos para a interface do ar, consoante a frequência empregue, para ser globalmente aceite;
- ISO 18000- 2: Para frequências abaixo dos 135 KHz;
- ISO 18000- 3: Para a frequência de 13,56 MHz;
- ISO 18000- 4: Para a frequência de 2,45 GHz;
- ISO 18000- 5: Para a frequência de 5,8 GHz;
- ISO 18000- 6: Para frequências entre os 860 aos 960 MHz;
- ISO 18000- 7: Para a frequência de 433 MHz.

NORMAS EPC Global:

- Classe 1: etiqueta simples, do tipo passiva, programável uma única vez e somente de leitura por retro-espalhamento com memória não volátil;
- Classe 2: etiqueta que comunica por retro-espalhamento com até 65 KB .

Anexo B: Tabelas referentes aos diversos comandos do módulo TRF7960EVM

Tabela B.1: Endereço de solicitação para habilitação do modo do receptor.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote	0x09	Tamanho do pacote = 9 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando de *firmware*	0xF1	AM/PM *toggle*
AM	0xFF	FF = AM e 00 = PM
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **0109000304F1FF0000**		

Tabela B.2: Endereço de solicitação do comando de inventário.

Endereço de solicitação		
Campo	**Conteudo**	**Observações**
SOF	0x01	Início da *frame*
Tamanho do pacote (dados)	0x0B	Tamanho = 11 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando do *firmware*	0x14	Pedido de inventário
Flags	0x06	*High data rate* = 1
Comando Anticolisão	0x01	
Tamanho da mascara	0x00	
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010B0003041406010000000**		

Tabela B.3: Endereço de solicitação para leitura de um único bloco da memória da etiqueta.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho de pacote (dados)	0x0B	Tamanho do pacote = 11 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando do *firmware*	0x18	*Request mode*
Flags	0x02	*Opção de flag* = 0; *High data rate* = 1
Comando para leitura de único bloco	0x20	
Numero do bloco selecionado	0x02	
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010B000304180220020000**		

Tabela B.4: Endereço de resposta da etiqueta a solicitação do comando “Read Single Block”.

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
0x40E	Fim de recepção
0x00	Etiqueta sem erros
0x11 0x11 0x11 0x11	Dados do block da etiqueta (32 bits)
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E0011111111**	

Tabela B.5: Endereço de solicitação para escrita de um único bloco da memória da etiqueta.

Endereço de solicitação		
Campo	**Conteudo**	**Observações**
Início of *frame*	0x01	Inicio da *frame*
Tamanho do pacote (dados)	0x0F	Tamanho do pacote = 15 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando do *firmware*	0x18	*Request mode*
Flags	0x42	*Option flag*=1; *High Data Rate flag*=1
Comando "*Write Single Block*"	0x21	Comando "*Write Single Block*"
Número do bloco selecionado	0x02	Bloco nº2, que corresponde ao nº3
Bloco de dados	0x11 0x11 0x11 0x11	32 bits
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010F000304184221021111111110000**		

Tabela B.6: Endereço de resposta da etiqueta a solicitação do comando "Write Single Block".

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
0x40E	Fim de recepção
0x00	Etiqueta sem erros
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E00**	

Tabela B.7: Endereço de solicitação para proteger um bloco da memória da etiqueta contra a escrita.

Endereço de solicitação		
Campo	**Conteudo**	**Observações**
Início of *frame*	0x01	Início da *frame*
Tamanho do pacote (dados)	0x0B	Tamanho do pacote = 11 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia a carga de dados
Comando do *firmware*	0x18	*Request mode*
Flags	0x40	*Option flag*=1; *High Data Rate flag*=0
Comando "Lock Block"	0x22	Comando "*Lock Block*"
Número do bloco selecionado	0x02	Bloco nº2, que corresponde ao nº3
Bloco de dados	0x11 0x11 0x11 0x11	32 bits
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010B000304184022021111111110000**		

Tabela B.8: Endereço de resposta da etiqueta a solicitação do comando "Lock Block".

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
[]	Sem resposta da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T[]**	

Tabela B.9: Endereço de solicitação para escrita de múltiplos blocos da memória da etiqueta.

Endereço de solicitação		
Campo	**Valor**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0F	Tamanho do pacote = 10 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	*Request* mode
Flags	0x42	*Option flag*= 1; *High data rate flag*= 1
Comando para escrita de um único bloco	0x21	Executa várias vezes o comado de escrita de um único bloco
Numero do bloco	0x02	Bloco 0x02 que corresponde ao bloco #3
	0x03	Bloco 0x03 que corresponde ao bloco #4
	0x04	Bloco 0x04 que corresponde ao bloco #5
Dados dos blocos	0x11 0x11 0x11 0x11	Dados contidos no bloco #3
	0x00 0x00 0x00 0x00	Dados contidos no bloco #4
	0x22 0x22 0x22 0x22	Dados contidos no bloco #5
Fim da *frame*	0x00 0x00	Fim da *frame*

Endereço de solicitação de escrita em Multiplos blocos, composto pela junção dos campos anteriores, presentes nesta tabela:

010F000203184221021111111100 (Bloco #3)

010F000203184221030000000000 (Bloco #4)

010F000203184221042222222200 (Bloco #3)

Tabela B.10: Endereço de resposta da etiqueta a solicitação do comando "Write Multiple Blocks".

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
40E	Fim de recepção
[00]	Etiqueta sem erro
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E[00]**	

Tabela B.11: Endereço de solicitação para silenciar uma etiqueta.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0A	Tamanho é de 10 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x00	Nenhuma *flag* selecionada
Comando "Stay Quiet"	0x02	
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010A0003041800020000**		

Tabela B.12: Endereço de resposta da etiqueta a solicitação do comando "Stay Quiet".

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
[]	Sem resposta da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T[00]**	

Tabela B.13: Endereço de solicitação para colocar etiqueta no modo de seleccionado.

Endereço de solicitação		
Campo	**Conteúdo**	***Observações***
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x12	Tamanho é de 12 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x20	A flag "Addressed" é selecionada
Comando "Select"	0x25	
UID	0x8C 0xAC 0xD6 0x06 0x00 0x00 0x07 0xE0	UID bytes estão invertidos
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **0112000304182025 8CACD606000007E0**		

Tabela B.14: Endereço de resposta da etiqueta a solicitação do comando “Select”.

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
[]	Sem resposta da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T[]**	

Tabela B.15: Endereço de solicitação para colocar etiquetas novamente em modo “Ready”.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0A	Tamanho é de 10 bytes
Constante	0x00	Constante
Início de carga de dados	0x03 0x04	Inicia carga de dados
Comando do *firmware*	0x18	Modo de solicitação
Flags	0x02	*Option flag*=1, *High data rate*=1
Comando “*Reseat to Ready*”	0x26	
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010A0003041802260000**		

Tabela B.16: Endereço de resposta da etiqueta a solicitação do comando "Reset to Ready"

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
40E	Fim de recepção
[00]	Etiqueta sem erro
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E[00]**	

Tabela B.17: Endereço de solicitação para modificar o registo AFI.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0B	Tamanho é de 11 bytes
Constante	0x00	Constante
Início de carga de dados	0x03 0x04	Inicia carga de dados
Comando *firmware*	0x18	Modo de solicitação
flags	0x42	*Option flag*=1; *High data rate flag*=1
Comando "*Write* AFI"	0x27	
AFI	0x05	AFI: 05=aplicações médicas
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010B03041827050000**		

Tabela B.18: Endereço de resposta da etiqueta a solicitação do comando "Write AFI".

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
40E	Fim de recepção
[00]	Etiqueta sem erro
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E[00]**	

B.19: Endereço de solicitação para proteger o registo AFi contra a escrita.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0A	Tamanho do pacote é de 10 bytes
Constante	0x00	
Início de carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x42	*Option flags*=1; *High data rate flags*=1
Comando "*Lock* AFI"	0x28	
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010A0003031842280000**		

Tabela B.20: Endereço de resposta da etiqueta a solicitação do comando "Lock AFI".

Resposta da etiqueta à solicitação	
Valor	**Observações**
80T	Fim de tansmissão
[]	Sem resposta da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T[]**	

Tabela B.21: Endereço de solicitação para modificar o registo DSFID.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Iniíio da *frame*
Tamanho do pacote de dados	0x0B	Tamanho do pacote de dados é 11 bytes
Constante	0x00	
Início de carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x42	Option *flag*=1; *High data rate*=1
Comando "Write DSFID"	0x29	
Valor DSFID	0x18	Formato de armazenamento de ID
Fim da *frame*	0x00 0x00	Fim da f*rame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010B000304184229180000**		

Tabela B.22: Endereço de resposta da etiqueta a solicitação do comando "Write DSFID".

Resposta da etiqueta à solicitação	
Conteúdos	**Observações**
80T	Fim de tansmissão
40E	Fim de recepção
[00]	Sem resposta da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E[00]**	

Tabela B.23: Endereço de solicitação para proteger o registo DSFIS das etiquetas contra a escrita.

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0A	O tamanho é de 10 bytes
Constante	0x00	
Início da carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x42	Opção *Flag option*=1;Opção *High data rate* =1
Comando "*Lock DSFID*"	0x2A	
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010A00030418422A0000**		

Tabela B.24: Endereço de resposta da etiqueta a solicitação do comando "Lock DSFID".

Resposta da etiqueta à solicitação	
Conteúdo	**Observações**
80T	Fim de tansmissão
01N	Sem interrupção de r
[00]	Sem resposta da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T01N[00]**	

B.25: Endereço de solicitação para correr o comando "Get System Info".

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	
Tamanho do pacote de dados	0x0A	O tamanho do pacote é de 10 bytes
Constante	0x00	
Início da carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x02	Opção flag=0; *High data rate flag*=1
Comando "*Get System Info*"	0x2B	
Fim da *frame*	0x00 0x00	
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010A00030418022B0000**		

Tabela B.26: Endereço de resposta da etiqueta a solicitação do comando "Get System Info".

Resposta da etiqueta à solicitação		
Campo	**Conteudo**	**Observações**
Fim de transmissão	80T	
	0x60F	Recepção do *buffer* de dados, 75% cheio
Fim de recepção	0x40E	Fim de recepção de dados
Flag de erro da etiqueta	0x00	Etiqueta sem erros
Flag de informação da etiqueta	0x0F	Campo de referencia, identificação da etiqueta Campo de memoria da etiqueta Campo AFI da etiqueta Campo DSIFD da etiqueta
UID da etiqueta	6EADD606000007E0	Em ordem invertida
Valor DSIFD da etiqueta	0x00	
Valor AFI da etiqueta	0x00	
Outros campos da etiqueta	0x3F 0x03 0x88	Número de blocos=64 Tamanho do bloco=32 bits Definido pelo fabricante da etiqueta
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T60F40E [00F6EADD606000007E000003F0388]**		

Tabela B.27: Endereço de solicitação para correr o comando "Get Multiple-Block Security Status"

Endereço de solicitação		
Campo	**Conteúdo**	**Observações**
Início da *frame*	0x01	Início da *frame*
Tamanho do pacote de dados	0x0C	Tamanho de pacote é de 12 bytes
Constante	0x00	Constante
Início da carga de dados	0x03 0x04	Inicia carga de dados
Comando de *firmware*	0x18	Modo de solicitação
Flags	0x02	Option *flag option*=0; *High data rate flag*=1
Commando " *Get Multiple Block Security Status*"	0x2C	
Numero do 1º bloco a bloquear	0x01	Bloco 01 que equivale na realidade ao bloco #2
Número de blocos (a bloquear)	0x02	Neste caso, serão bloqueados os 3 seguintes blocos
Fim da *frame*	0x00 0x00	Fim da *frame*
Endereço de solicitação deste comando, composto pela junção dos campos anteriores presentes nesta tabela: **010C00030418022C01020000**		

Tabela B.28: Endereço de resposta da etiqueta a solicitação do comando "Get Multiple-Block Security Status".

Resposta da etiqueta à solicitação	
Conteudo	**Observações**
80T	Fim de transmissão
0x40E	Fim de recepção
0x00	Etiqueta sem erros
0x00	Estado de segurança do bloco #1
0x00	Estado de segurança do bloco #2
0x00	Estado de segurança do bloco #3
Endereço de resposta da etiqueta, ao comando, composta pela junção dos campos desta tabela: **80T40E[00000000]**	