

## Desenvolvimento de Sistema para Controlo de um Quarto de Hotel

**MANUEL FERNANDO MOREIRA DA SILVA**

novembro de 2016

# DESENVOLVIMENTO DE SISTEMA PARA CONTROLO DE UM QUARTO DE HOTEL

Manuel Fernando Moreira da Silva



Departamento de Engenharia Eletrotécnica  
Mestrado em Engenharia Eletrotécnica e de Computadores  
Área de Especialização em Automação e Sistemas

**2016**



Relatório elaborado para satisfação parcial dos requisitos da Unidade Curricular de  
Tese/Dissertação do Mestrado em Engenharia Eletrotécnica e de Computadores

Candidato: Manuel Fernando Moreira da Silva, N° 1100450, [1100450@isep.ipp.pt](mailto:1100450@isep.ipp.pt)

Orientação científica: Lino Manuel Baptista Figueiredo, [lbf@isep.ipp.pt](mailto:lbf@isep.ipp.pt)

Empresa: ISEP - GECAD

Supervisão: António José Matos de Meireles, [ajmme@isep.ipp.pt](mailto:ajmme@isep.ipp.pt)



Departamento de Engenharia Eletrotécnica  
Mestrado em Engenharia Eletrotécnica e de Computadores  
Área de Especialização em Automação e Sistemas

**2016**



## *Agradecimentos*

À minha família, namorada e amigos pelo apoio incondicional ao longo deste percurso.

Ao Dr. Lino Figueiredo e Engenheiro António Meireles, meus orientadores pelo apoio e total disponibilidade durante o projeto.



## *Resumo*

O setor hoteleiro atualmente tem necessidade de estar em linha com as evoluções tecnológicas, fazendo uso das mesmas de forma a aumentar o nível de serviço e qualidade para os hóspedes.

O projeto geral Smart Hotel visa apresentar uma solução global de controlo de um hotel, com interação do hóspede, desde de uma aplicação android até ao sistema de gestão.

O projeto desenvolvido visa desenvolver o controlo de acesso ao quarto de um hotel como também o controlo dos diferentes periféricos no interior do quarto, com recurso ao *smartphone*.

O sistema desenvolvido está dividido em dois módulos, o módulo da fechadura e o módulo central, no qual utilizam microcontroladores PIC para todo o seu controlo. O acesso ao quarto é realizado através de um *smartphone* com NFC, esta leitura é realizada no módulo da fechadura, que por sua vez valida a autorização de entrada com o módulo central, esta comunicação entre os dois módulos é por ZigBee. No interior do quarto, o hóspede pode fazer o controlo da iluminação, ar condicionado, televisão e ainda dos estores através do *smartphone*, que comunica com o módulo central por *Bluetooth*. Por sua vez o módulo central possui uma ligação *Ethernet* de forma a estar sempre ligado ao servidor do hotel.

Todo o sistema desenvolvido foi pensado com o objetivo de permitir ser instalado em hotéis que possuam outras soluções antigas, e de forma a que os custos de instalação sejam baixos, tornando a solução interessante.

### *Palavras-Chave*

*Smartphone*, NFC, ZigBee, *Bluetooth*, *Ethernet*, Microcontrolador - PIC



## *Abstract*

Nowadays the hotel industry needs to be in line with technological developments, making use of them in order to increase the level of service and quality for guests.

The goal of the project is develop global solution for the control of a hotel, with guest interaction, since an android application to the management system.

The aim of the project is to develop a user-friendly system to interact with the room control system of a hotel using a smartphone.

The developed system is based on PIC microcontroller and is divided in two modules, the door lock module and the central module. The door module is used to unlock via a smartphone with NFC. Inside the room, guests can control lighting, air conditioning, television and even the blinds through the phone, which communicates with the central module via Bluetooth. The central module also has an Ethernet connection in order to be always connected to the hotel server.

The developed system has been designed with the aim to be installed in hotels that have other solutions, in order to have low setup costs.

### ***Keywords***

*Smartphone, NFC, ZigBee, Bluetooth, Ethernet, Microcontroller - PIC*



# Índice

<b>AGRADECIMENTOS</b> .....	<b>I</b>
<b>RESUMO</b> .....	<b>III</b>
<b>ABSTRACT</b> .....	<b>V</b>
<b>ÍNDICE</b> .....	<b>VII</b>
<b>ÍNDICE DE FIGURAS</b> .....	<b>IX</b>
<b>ÍNDICE DE TABELAS</b> .....	<b>XIII</b>
<b>ACRÓNIMOS</b> .....	<b>XV</b>
<b>1. INTRODUÇÃO</b> .....	<b>1</b>
1.1. CONTEXTUALIZAÇÃO .....	1
1.2. OBJETIVOS .....	3
1.3. CALENDARIZAÇÃO .....	4
1.4. ORGANIZAÇÃO DO RELATÓRIO .....	5
<b>2. ESTADO DA ARTE</b> .....	<b>7</b>
2.1. TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO .....	7
2.2. REDES DE COMUNICAÇÃO SEM FIOS .....	10
2.3. TECNOLOGIA ZIGBEE .....	12
2.4. TECNOLOGIA BLUETOOTH .....	20
2.5. TECNOLOGIA NFC – NEAR FIELD COMMUNICATION .....	26
2.6. TECNOLOGIA ETHERNET.....	31
<b>3. ARQUITETURA GERAL</b> .....	<b>35</b>
3.1. ENQUADRAMENTO PROJETO <i>SMART HOTEL</i> .....	35
3.2. ARQUITETURA GERAL DO PROJETO <i>SMART HOTEL</i> .....	36
3.3. REQUISITOS DO SISTEMA MÓDULO CONTROLO DO QUARTO .....	38
3.4. ARQUITETURA MÓDULO FECHADURA .....	38
3.5. ARQUITETURA MÓDULO CENTRAL.....	40
3.6. ARQUITETURA DE SOFTWARE.....	41
<b>4. DESENVOLVIMENTO</b> .....	<b>43</b>
4.1. MÓDULO FECHADURA .....	44
4.2. MÓDULO CENTRAL.....	57
<b>5. CONCLUSÕES</b> .....	<b>82</b>
5.1. TRABALHOS FUTUROS .....	83

<b>REFERÊNCIAS DOCUMENTAIS.....</b>	<b>84</b>
<b>ANEXO A. PCB – MÓDULO FECHADURA.....</b>	<b>88</b>
<b>ANEXO B. PCB – MÓDULO CENTRAL.....</b>	<b>89</b>

## Índice de Figuras

Figura 1	Estrutura de uma rede <i>Wireless</i> [4].....	12
Figura 2	Comparação entre as diferentes Tecnologias [13].....	14
Figura 3	Tipos de dispositivos físicos numa rede ZigBee [13] .....	15
Figura 4	Topologia de rede em Estrela.....	16
Figura 5	Topologia de rede em Malha.....	17
Figura 6	Topologia de rede em Árvore.....	17
Figura 7	Topologias de Rede [16] .....	21
Figura 8	Pilha de Protocolos [17].....	22
Figura 9	Hardware Bluetooth [17].....	24
Figura 10	Diagrama de Estados [19] .....	25
Figura 11	Modos de Operação NFC [22] .....	30
Figura 12	Versões de Frame [26] .....	33
Figura 13	Arquitetura Geral – Smart Hotel .....	37
Figura 14	Arquitetura Módulo Fechadura .....	39
Figura 15	Montagem de Fechadura .....	39
Figura 16	Arquitetura Módulo Central .....	40
Figura 17	Arquitetura <i>Software</i> Módulo Fechadura .....	41
Figura 18	Arquitetura <i>Software</i> Módulo Central .....	42
Figura 19	Arquitetura Módulo Fechadura .....	44
Figura 20	Módulo NFC – RC552 .....	46
Figura 21	Módulo ZigBee – Xbee .....	47
Figura 22	Descrição dos Pinos do Módulo XBee.....	47
Figura 23	Circuito Elétrico Módulo Fechadura.....	48
Figura 24	Montagem do circuito elétrico do módulo Fechadura.....	50
Figura 25	Montagem do módulo Fechadura em PCB .....	52
Figura 26	Fluxograma do programa principal do módulo Fechadura .....	53
Figura 27	Trama de dados no modo API.....	54
Figura 28	Fluxograma do serviço de interrupções do módulo da fechadura .....	56
Figura 29	Arquitetura do Módulo Central .....	57
Figura 30	Circuito multiplexer da USART, adaptado de [30].....	59
Figura 31	Módulo Bluetooth HC-06.....	61
Figura 32	Montagem do ENC28J60 [33] .....	62
Figura 33	Módulo Ethernet – ENC28J60 .....	63
Figura 34	Circuito Elétrico Módulo Central – Circuito Central .....	63

Figura 35	Circuitos de Potência - a) Circuito Relé b) Circuito TRIAC.....	65
Figura 36	Circuito Elétrico Módulo Central – Circuito Ethernet .....	65
Figura 37	Montagem do Circuito Elétrico do Módulo Central – Circuito Central.....	67
Figura 38	Montagem do Circuito Elétrico do Módulo Central – Circuito Ethernet .....	67
Figura 39	Montagem Total do Circuito Elétrico do Módulo Central .....	68
Figura 40	Montagem do módulo Central em PCB .....	69
Figura 41	Fonte de Alimentação para calha DIN, adaptado de [31].....	70
Figura 42	Fluxograma do programa principal do PIC 18F2550.....	71
Figura 43	Fluxograma do Serviço de Interrupção da USART PIC 18F2550 .....	74
Figura 44	Fluxograma do serviço das interrupções externas PIC 18F2550.....	75
Figura 45	Fluxograma do programa principal PIC 18F4620.....	76
Figura 46	Fluxograma do serviço de interrupção PIC 18F4620.....	78
Figura 47	Web server – Smart Hotel .....	79
Figura 48	Fluxo Geral de Comunicação .....	80
Figura 49	Fluxo de Comunicação do Smartphone.....	81





## *Índice de Tabelas*

Tabela 1	Calendarização do Projeto.....	4
Tabela 2	Configurações da comunicação [24] .....	27
Tabela 3	Combinação dos modos Ativo/Passivo como Iniciador/Destino [24].....	28
Tabela 4	Seleção de Canal MAX 399 .....	60
Tabela 5	Pinos de ligação do módulo HC-06.....	61



## *Acrónimos*

AC	–	Alternating Current
API	–	Application Programming Interface
APs	–	Access Points
CMOS	–	Complementary Metal-Oxide-Semiconductor
CS	–	Chip Select
CSMA/CD	–	Carrier Sense Multiple Access/Collision Detect
CSMA/CA	–	Carrier Sense Multiple Access/Collision Avoidance
DEC	–	Digital Equipment Corporation
DI	–	Data In
DIN	–	Deutsches Industrie Norm
DMA	–	Direct Memory Access
DO	–	Data Out
ED	–	End Devices
EN	–	Enable
EUSART	–	Enhanced Universal Synchronous Asynchronous Receiver Transmitter
FFD	–	Full Function Devices
FHS	–	Frequency Hopping-Synchronization
FSM	–	Finite State Machine

GND	– Ground
HTTP	– Hypertext Transfer Protocol
I <sup>2</sup> C	– Inter-Integrated Circuit
ICSP	– In-Circuit Serial Programming
IEEE	– Institute of Electrical and Electronics Engineers
IFF	– Identify Friend or Foe
INT	– Interruption
ISM	– Industrial Scientific and Medical
ISO/IEC	– International Organization for Standardization/International Electrotechnical Commission
JIS	– Japanese Industrial Standard
L2CAP	– Logical Link Control and Adaptation
LAN	– Local Area Network
LLCP	– Logical Link Control Protocol
LSB	– Least Signification Byte
MAC	– Media Access Control
MAN	– Metroplitan Area Network
MANET	– Mobile Area Network
MSB	– Most Signification Byte
MSSP	– Master Synchronous Serial Port
NCI	– NFC Control Interface

NDEF	– NFC Data Exchange Format
NFC	– Near Field Communication
NFCIP	– Near Field Communication Interface Protocol
NWK	– Network
OSI	– Open Systems Interconnection
PCB	– Printed Circuit Board
PGC	– Programming Clock
PGD	– Programming Data
PHY	– Physical
PIC	– Programmable Interrupt Controller
PPP	– Point-to-Point Protocol
RAM	– Random Access Memory
RF	– Radio Frequency
RFD	– Reduced Function Devices
RFID	– Radio-Frequency Identification
RTD	– Record Type Definition
RX	– Reception
SCK	– Serial Clock
SDI	– Serial Data Input
SDO	– Serial Data Output
SIG	– Special Interest Group

SPI	–	Serial Peripheral Interface
SSP	–	Security Service Provider
TCP/IP	–	Transmission Control Protocol/Internet Protocol
TRIAC	–	Triode for Alternating Current
TX	–	Transmission
UART	–	Universal Asynchronous Receiver Transmitter
UDP	–	User Datagram Protocol
UPC	–	Unidade de Processador Central
UPE	–	Unidade de Processador da Ethernet
UPF	–	Unidade de Processador da Fechadura
URIs	–	Uniform Resource Identifiers
USART	–	Universal Synchronous Asynchronous Receiver Transmitter
V <sub>in</sub>	–	Voltage input
WAP	–	Wireless Application Protocol
WLAN	–	Wireless Local Area Network
WMAN	–	Wireless Metroplitan Area Network
WPAN	–	Wireless Personal Area Network
WWAN	–	Wireless Wide Area Network





# 1. INTRODUÇÃO

O presente relatório pretende apresentar o trabalho elaborado como Tese/Dissertação, do 2º ano de Mestrado em Engenharia Eletrotécnica e Computadores (MEEC), do Departamento de Engenharia Eletrotécnica (DEE), do Instituto Superior de Engenharia do Porto. O trabalho elaborado rege-se no desenvolvimento de um sistema para controlo de um quarto de hotel através de um *smartphone*, onde é possível o controlo de iluminação, aquecimento e acesso ao quarto do hotel, através da tecnologia sem fio, no qual, é realizada uma contextualização sobre o tema apresentado e esclarecer as tendências da aplicação da tecnologia na hotelaria. Também serão identificados os objetivos principais realizando uma pequena interligação com os requisitos necessários de modo a desenvolver o trabalho final.

## 1.1. CONTEXTUALIZAÇÃO

Nos últimos anos tem-se assistido a uma enorme expansão de dispositivos que comunicam através da tecnologia sem fio, que surgem nas mais diversas áreas, ocupando um espaço cada vez mais significativo no quotidiano das pessoas e empresas. A ausência de uma ligação por cabo e uma consequente versatilidade em termos de instalação ou posição dos dispositivos intervenientes na rede que se apoiam sobre este tipo de comunicação, a acrescentar à possibilidade dos próprios emissores ou recetores poderem estar em movimento durante a comunicação.

A evolução da tecnologia sem fio está relacionada com o avanço tecnológico ocorrido na área dos microprocessadores, na área dos sensores e na área de armazenamento de energia

com a criação de novos e mais pequenos dispositivos, permitiram o aparecimento de uma nova área de desenvolvimento, as redes de sensores sem fios.

As redes de sensores sem fios atualmente estão a ser cada vez mais utilizadas em diversas áreas de aplicação, como por exemplo para uso militar, monitorização ambiental, domótica, automação industrial, entre outras.

A comunicação sem fios permite maior flexibilidade quando comunicam, pois não necessitam de permanecer numa localização fixa. As tecnologias sem fio tornam os serviços de comunicação mais facilmente disponíveis do que os tradicionais baseados em cabos instalados fisicamente. Os serviços sem fios permitem uma comunicação independente da sua localização.

Atualmente utilização de equipamentos móveis que utilizam a tecnologia de comunicação sem fio, tais como, *smartphone*, *tablet* e computador portátil é cada vez maior, e a tendência é o crescimento ainda mais acelerado nos próximos anos. A evolução da utilização dos equipamentos está bastante relacionada com o aumento da capacidade de processamento e armazenamento dos dispositivos móveis.

O crescimento da tecnologia e a facilidade com que hoje em dia se consegue aceder à internet através de dispositivos móveis (*smartphones* ou *tablets*) faz com que a mobilidade de informação seja rápida e eficaz, no qual cada vez mais o acesso à internet é constante. Os hotéis tendem a acompanhar o crescimento da tecnologia, o que leva a começarem a investir em redes sem fios profissionais de forma a garantir a cobertura total da área do hotel. Atualmente cada hóspede possui o seu próprio computador, *tablet* e *smartphone*, isto leva a que a rede sem fios do hotel esteja dimensionada para que no mínimo seja possível três ligações à rede por cada cliente.

A internet é cada vez mais utilizada, sendo a primeira ferramenta utilizada para a escolha dos hotéis, as plataformas hoteleiras (Booking, TripAdvisor) são muito utilizados, pois disponibilizam o feedback dos clientes assim como a comparação de preços com outros hotéis, uma boa ligação de internet tendencialmente leva a que as notas atribuídas nas plataformas aumentem.

Tipicamente os clientes dos hotéis procuram o acesso ao Wi-Fi em qualquer parte do hotel, assim como, procuram aplicações para *smartphones* de forma a completar a informação

sobre o hotel, sobre os pontos de interesse nos arredores e sobre a região onde se encontram hospedados.

Os consumidores no geral, estão cada vez mais ligados a dispositivos móveis, consequência disso a tendência dos hotéis é apostar numa tecnologia que permita abrir portas do quarto, fazer reservas, escolha do quarto, *check-in* e *check-out* através do *smartphone*.

## **1.2. OBJETIVOS**

O objetivo principal deste projeto é o desenvolvimento de um sistema capaz de controlar um quarto de hotel, desde do controlo de acesso, controlo de iluminação, ar condicionado, televisão e ainda a interligação com o sistema de gestão do hotel. Para responder ao objetivo principal do projeto foram definidas pelo orientador múltiplas tarefas mais simplificadas, de forma a estruturar e organizar o projeto, tais como:

- Controlo de acesso através do *smartphone* através de NFC;
- Comunicação com *smartphone* através de Wi-Fi e *Bluetooth*;
- Estabelecer ligação *Ethernet* com servidores do hotel;
- Controlo de diferentes elementos do quarto (Iluminação, TV, A/C, Estores);

### 1.3. CALENDARIZAÇÃO

Para o desenvolvimento da solução existiu a necessidade de realizar um planeamento progressivo de todas as tarefas principais a serem desenvolvidas ao longo do projeto. Este planeamento encontra-se apresentado na Tabela 1 onde é possível verificar os tempos previstos a serem gastos em cada uma das tarefas.

**Tabela 1** Calendarização do Projeto

Descrição	Plano										
	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov
Tecnologias e sistemas correntes	■	■									
Estudo tecnologias utilizadas		■	■								
Identificação dos requisitos		■	■	■							
Definição de arquitetura				■	■	■					
Implementação					■	■					
Testes					■	■	■				
Prototipagem							■	■	■		
Documentação		■	■	■					■	■	■

#### **1.4. ORGANIZAÇÃO DO RELATÓRIO**

No Capítulo 1 é apresentada uma breve introdução ao trabalho desenvolvido bem como uma contextualização do tema de uma forma geral, assim como, também os objetivos que são pretendidos com a execução do trabalho e por último a planeamento do mesmo.

No Capítulo 2 é descrito todas as tecnologias presente na elaboração do trabalho, desde das características e especificações das diferentes tecnologias que iram constituir o trabalho e uma breve referência aos aspetos gerais das redes sem fios.

No Capítulo 3 é apresentado o projeto desenvolvido de uma perspectiva geral, bem como a decomposição do projeto em dois módulos principais, para cada um dos módulos é apresentado os aspetos principais a arquitetura do *hardware* e de *software*.

No Capítulo 4 é descrito as várias fases de desenvolvimento do projeto, este capítulo também está dividido nos dois módulos do projeto, no qual em cada um é explicado ao detalhe o *hardware*, desde arquitetura, componentes, circuito elétrico, montagem e ainda a prototipagem de cada um dos módulos e ainda é documentado todo o *software* desenvolvido para os microcontroladores.

No Capítulo 5 é a conclusão de todo o trabalho realizado e documentado, neste capítulo é apresentado os trabalhos futuros para este projeto no sentido de evolução da solução.



## 2. ESTADO DA ARTE

Este capítulo pretende apresentar conceitos fundamentais para o desenvolvimento do trabalho. Todos os conceitos aqui abordados são importantes para a compressão das opções tomadas durante a realização do projeto. Aqui são apresentadas algumas soluções de controlo para hotéis, assim como, características das redes sem fios e também serão abordadas as tecnologias de comunicações presentes no trabalho.

### **2.1. TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO**

Atualmente o setor das tecnologias de informação e comunicação esta marcado pelo seu rápido desenvolvimento e crescimento em vários setores de atividade. Esta evolução incrementa valor aos produtos e serviços, elevando o seu conteúdo tecnológico, permitindo uma evolução constante dos produtos/serviços.

A utilização da tecnologia de informação é inevitável em qualquer empresa moderna, atualmente o computador é uma das tecnologias mais populares e eficazes que temos ao dispor para trabalhar a informação digital.

No setor hoteleiro as estruturas tecnológicas de informação que os hotéis possuem são essencialmente o website, intranet e a gestão integrada de segurança, estando em constante

avanço e evolução, o uso adequado da tecnologia que permita aumentar o conforto e a excelência dos serviços prestados.

### **2.1.1. SISTEMAS DE CONTROLO EM QUARTOS DE HOTÉIS– ATUALIDADE**

Atualmente em Portugal, os sistemas de controlo presentes nos quartos de hotel são sistemas independentes entre si e com pouco cruzamento de informação. A gestão e controlo de acesso nos hotéis nacionais de quatro estrelas é realizada através de sistema de controlo de acesso RFID (*Radio-Frequency Identification*) MIFARE, trata-se de uma fechadura eletromecânica de utilização simples, este sistema utiliza cartões de proximidade MIFARE.

Aquando da entrada nos quartos de hotel, o cartão é colocado no suporte elétrico de parede junto da entrada do quarto, funciona como interruptor geral de quarto, ou seja, qualquer sistema elétrico só funciona com o cartão inserido no suporte. Na saída do quarto, se o cartão for removido do suporte todos os periféricos do quarto são desligados.

O ar condicionado é por norma controlado no interior do quarto através de um controlador, regra geral estes controladores ficam perto da entrada do quarto. Estes aparelhos só funcionam quando o hóspede está no quarto caso saia e retire o cartão do suporte o ar condicionado é desligado, não é possível manter a temperatura no quarto durante a saída do hóspede do quarto por um pequeno espaço de tempo.

O controlo da iluminação na maioria dos casos é o sistema tradicional interruptores na entrada do quarto, na entrada da casa de banho e junto da cama do quarto, por vezes os pontos de iluminação do quarto são projetores de iluminação direta. Contudo em hotéis mais evoluídos a iluminação é indireta e permite ser regulada. Em alguns casos os hotéis estão equipados com sistemas de domótica.

Em Portugal, atualmente os hotéis ainda não disponibilizam aos hóspedes aplicações móveis para o controlo de sistemas nos quartos de hotéis. O processo de *check-in* é o tradicional, o hóspede dirige-se á receção, qual deve fazer o registo dos seus dados e lhe é fornecido a “chave” do quarto, um cartão MIFARE, de seguida o hóspede desloca-se para o quarto e apenas no seu interior pode controlar todos os periféricos. A maioria dos hotéis já dispõem de acesso Wi-Fi em todo o hotel. A comunicação entre o hóspede e a receção é sempre realizado por telefone do quarto.

### 2.1.2. SOLUÇÕES EXISTENTES PARA HOTÉIS

Atualmente os hotéis apostam cada vez mais nas novas tecnologias de forma a dar respostas às necessidades dos clientes cada vez mais exigentes. O acesso gratuito ao Wi-Fi é uma necessidade e exigência dos clientes, normalmente cada cliente possui vários equipamentos com necessidade frequentes de ligação à internet.

Em Portugal existem várias empresas com soluções *smart*, de forma a aumentar a satisfação do cliente e a eficiência do hotel, soluções distintas com áreas de atuação diferentes, desde da receção até à tecnologia e sistemas disponíveis nos quartos de hotel. [28]

Kiosk self-service [28], solução lançada pela empresa SoftConcept, é uma solução que consiste em substituir a receção do hotel num “*kiosk*” que permitirá fazer *check-in*, *check-out*, pagamentos, atribuição da chave do quarto, entre outras tarefas. Este sistema visa reduzir as filas de espera na receção do hotel, aumentando o conforto dos clientes. A solução diminui o número de pessoal, uma vez que a atendimento é automático. O *kiosk self-service* possui outros benefícios para os clientes que possuem cartão e fidelização, este cartão vai ser codificado para ser utilizado para abrir a porta do quarto.

InovGuest [28], solução de gestão hoteleira da empresa Warenguest, trata-se de uma plataforma que integra todo tipo de periféricos, pois o mesmo “gere interfaces com *scanners* de documentos, vídeo On Demand/Pay TV, gravadores de cartões de fechaduras, entre outros” (Paulo Lopes, *Sales manager* da Warenguest). Esta solução integra a informação tornando-a acessível num único ponto, permitindo a diminuição de pessoal na receção, visa a redução do tempo de espera no *check-in/check-out*.

Set-top box solução da empresa Nonius [28], combina o serviço TV e filmes de alta definição com acesso a internet, disponibilizando um excelente acesso a internet e qualidade de imagem na TV. A solução combina vários serviços num único sistema e responde ainda aos desafios “*green*” do hotel, pois esta disponível na TV do quarto do hóspede todo material de comunicação de hotel.

DirectClick [28] da empresa Availpro é uma solução que permite aos hotéis aparecerem em sites de comparação de preços como trivago, KelKoo. Com esta solução permite ao hotel ser escolhido com o melhor preço disponível entre outros canais. A empresa tem o foco nas soluções *on-line*.

## 2.2. REDES DE COMUNICAÇÃO SEM FIOS

O IEEE (*Institute of Electrical and Electronics Engineers*) é uma organização profissional sem fins lucrativos, tendo como objetivo o desenvolvimento tecnológico. Nesse sentido são realizadas muitas conferências e palestras, onde uma das funções de bastante destaque é a criação, aprovação e divulgação de normas técnicas que permitem normalizar as tecnologias abordadas [1].

Um das tecnologias desenvolvidas é a tecnologia *Wireless* (rede sem fios) que nos últimos anos tem inovado o setor das comunicações. Com o avanço tecnológico os custos de utilização da mesma foram reduzindo, tornando o seu uso e aplicações acessível. Existem diversas definições desta tecnologia, mas podemos definir *Wireless* como sendo uma tecnologia que disponibiliza a transmissão de dados, sem fazer uso de cabos, mas através de ondas de rádio frequência [2].

O uso de redes sem fio tornou-se essencial tanto em ambientes domésticos como nos ambientes empresariais onde é preciso ter mobilidade e ao mesmo tempo acessibilidade a recurso da rede como informação arquivada e acesso a *email* [3].

Esta tecnologia ao longo dos anos com a exigência dos mercados, está em crescimento constante, tornando-se num dos meios de comunicação mais utilizados, pois proporciona diversas funcionalidades tais como acesso a internet, comunicação entre aparelhos, um computador com uma impressora, entre inúmeras utilizações domésticas.

Existem diversos tipos de rede *Wireless* que serão abordadas no subcapítulo 2.2.1 seguindo todos a mesma camada protocolar. As redes sem fios possuem 5 camadas protocolares:

- Camada Física: onde se encontra os meios de conexão por onde irão navegar os dados a serem transmitidos, os componentes de *hardware* são incluídos nesta camada para transmissão da informação;
- Camada de ligação: nesta camada é onde se deteta e corrige os erros que possam acontecer na camada física, é aqui que é feito o controlo de fluxo e é este que estabelece um protocolo de comunicação entre os sistemas;

- Camada de rede: esta camada é responsável por realizar o controlo da operação da rede, é nesta camada que são feitos os encaminhamentos dos pacotes entre a fonte e o destino;
- Camada de transporte: é a camada responsável pela transferência eficiente, confiável e económica das informações a serem trocadas entre a máquina de origem e de destino;
- Camada de aplicação: é a camada responsável por dar auxílio a serviços para que as aplicações desenvolvidas entendam a informação trocada entre os computadores.

### 2.2.1. TIPO DE REDE WIRELESS

As redes sem fios são divididas em quatro grupos específicos [5], de acordo com as áreas de aplicação, o alcance do sinal e a taxa de transmissão de dados, estas são os principais critérios para a sua divisão. O grupo de redes sem fios são os seguintes:

- *Wireless Personal Area Network* (WPAN);
- *Wireless Local Area Network* (WLAN);
- *Wireless Metropolitan Area Network* (WMAN);
- *Wireless Wide Area Network* (WWAN).

A WPAN define tecnologias *Wireless* cujo alcance máximo dos sinais é de 10 metros. Estas redes caracterizam-se por ter baixa de transferência de dados e baixa potência. A possibilidade de ligação no modo *ad hoc*, modo que não utiliza infraestrutura, é uma das suas vantagens. A rede é tipicamente representada pela tecnologia *Bluetooth* de acordo com a norma IEEE 802.15.1 e pela tecnologia *ZigBee* de acordo com a norma IEEE 802.15.4.

A WLAN, refere-se à comunicação de equipamentos em áreas restritas (sala, edifício), esta tecnologia tem um alcance máximo de 100 metros, tendo como objetivo partilhar recursos computacionais. Com este tipo de rede é possível interligar edifícios sem que seja necessário a utilização de cabos para a transmissão de dados sendo esta realizada via rádio. Esta rede é normalmente representada pelo *Wi-Fi* de acordo com a norma IEEE 802.11. As redes WLAN operam em dois modos, modo infraestrutura (*Access Points* - APs) e no modo *ad hoc*.

A WMAN é uma rede de área metropolitana, e possui um alcance máximo de 5 km. Estas redes permitem altas velocidades de dados em comparação com a taxa de dados de tecnologia de telecomunicação móvel, bem como outras redes sem fios. O objetivo desta rede é o acesso de banda larga através de um único ponto linear.

A WWAN permite aceder a internet através de um cartão WWAN e um computador (por exemplo). Estas redes oferecem uma alta velocidade de dados e o seu alcance também é extenso. As redes de telefone móveis são um bom exemplo de WWAN, pois estas fornecem uma cobertura sem fios regional, nacional e global [5][6][7].

Na Figura 1 encontra-se apresentada a divisão dos 4 tipos de redes *Wireless*, fazendo ênfase às normas IEEE associadas para cada tipo de rede, assim como as diferentes distâncias e taxas de transmissão de envio de dados.

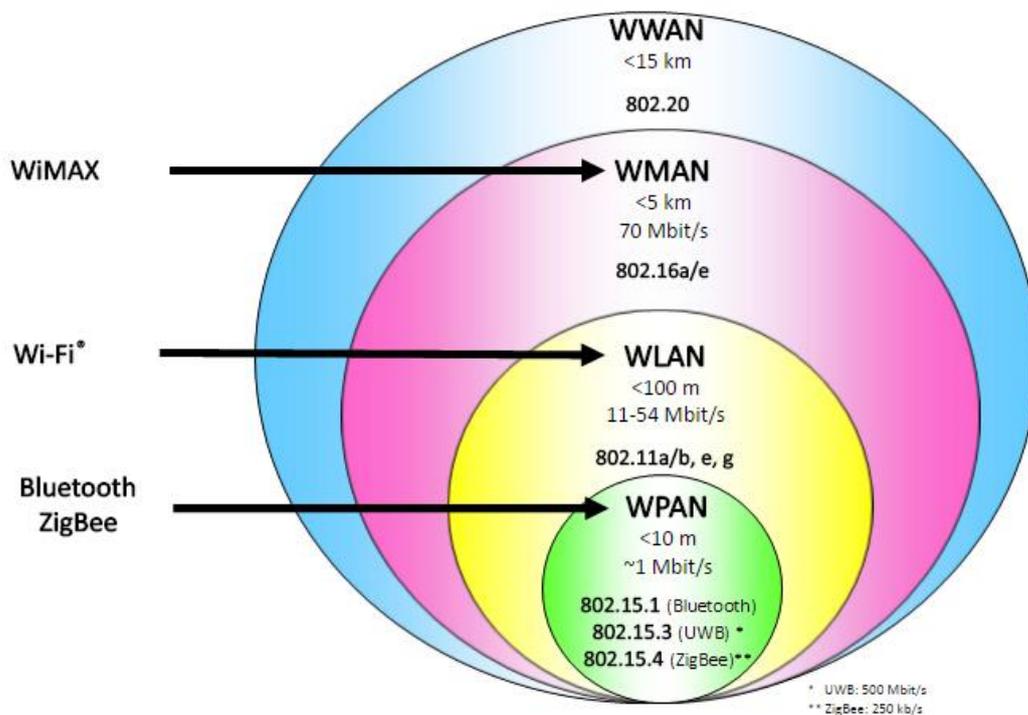


Figura 1 Estrutura de uma rede Wireless [4]

### 2.3. TECNOLOGIA ZIGBEE

Tal como foi analisado no subcapítulo 2.2.1, a tecnologia ZigBee é uma tecnologia sem fios que se encontra no grupo WPAN de acordo com a norma IEEE 802.15.4. O ZigBee apareceu por volta de 1998 [14] quando se começou a sentir que as tecnologias existentes tal como o

*Wi-Fi* e o *Bluetooth* não se conseguiram adaptar ao desenvolvimento de algumas aplicações. O ZigBee possui três características que diferenciam esta tecnologia das restantes:

- O consumo necessário para realizar transmissão de dados é bastante inferior face às restantes, funcionando com uma pilha durante bastante tempo (dependendo da aplicação desenvolvida);
- A possibilidade de comunicar entre diversos dispositivos é bastante abrangente, sendo o número de dispositivos existentes na rede elevado;
- A taxa de transmissão desta tecnologia é mais baixa sendo utilizado para transmitir dados que não são alterados com muita periodicidade.

Segundo a referência [12], esta tecnologia é bastante utilizada para aplicações de controlo e de monitorização devido à sua característica de não necessitar de cabelagem para troca de informação entre dispositivos consumindo pouca energia. O ZigBee é utilizado para desenvolver aplicações de automação, aplicações ligadas à área da saúde e também aplicações na área das telecomunicações.

Para realizar a comunicação a tecnologia ZigBee utiliza rádio frequência, existem 3 frequências disponíveis para realizar esta comunicação, 2.4 GHz (com taxa de transferência de dados de 250 kbps) que é o mais utilizado, 915 MHz (com taxa de transferência de dados de 40 kbps) e 868 MHz (com taxa de transferência de dados de 20 kbps) [15].

Tal como as restantes tecnologias sem fios as distâncias para transferir dados, depende de algumas características ambientais (obstáculos físicos, interferência eletromagnética entre outros). A tecnologia ZigBee foi pensada para trabalhar em distâncias curtas (inferiores a 10 metros), no entanto, dependendo do ambiente em questão possibilita alcances até a 100m (distância idêntica à das WLAN), no entanto as taxas de transmissão poderão ser diminuídas face ao funcionamento normal.

Na Figura 2 encontra-se uma comparação das diferentes tecnologias utilizadas para comunicação sem fios (ZigBee, *Bluetooth* e *Wi-Fi*), verificando que para as mesmas distâncias as três tecnologias têm comportamento diferentes relativamente às taxas de transmissão de dados.

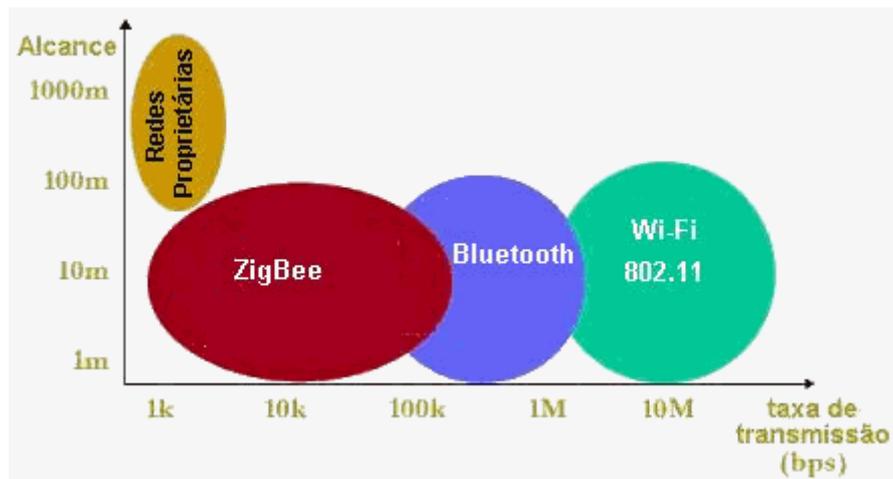


Figura 2 Comparação entre as diferentes Tecnologias [13]

O ZigBee possui uma configuração bastante simples, no entanto a simplicidade de configuração não o torna pouco segura para realizar a transferência de dados.

### 2.3.1. DISPOSITIVOS ZIGBEE

Tipicamente, numa rede ZigBee, existem dois tipos de dispositivos físicos denominados por *Full Function Device* (FFD) e o *Reduced Function Device* (RFD). Os FFD são dispositivos mais complexos e necessitam de um *hardware* mais potente para a implementação da pilha protocolar [10]. Sendo estes mais potentes realizam consumos de energia maiores, estes podem desempenhar a função de coordenador da rede e também conseguem comunicar com os restantes dispositivos (*Router's* ou *End Devices* - ED). A nível de *hardware* é implementado em microcontroladores com mínimo de 32 KB de memória de programa e alguma memória RAM (*Random Access Memory*) disponível para implementação das tabelas de rotas e de configuração de parâmetros. Os RFD são limitados, na topologia em estrela não podem funcionar como coordenador da rede, apenas tendo a possibilidade de comunicar com ele. A nível de *hardware* são mais simples face aos FFD, onde podem ser implementados com microcontroladores de 8 bits com uma memória de programa de 6 KB. Do ponto de vista de uma rede ZigBee estes só assumem o papel de *End Devices*. Face aos FFD, os RFD são fáceis de configurar uma vez que não possuem tantas funções disponíveis para controlar a rede tal como definir que dispositivos que estão na rede. Normalmente estes dispositivos são utilizados para controladores de relés, ligação de sensores, entre outros [13].

O protocolo ZigBee faz a distinção entre três dispositivos lógicos:

- Os coordenadores que são do tipo FFD têm como função configurar a rede e atribuir endereços aos dispositivos da rede (só existe um coordenador por cada rede);
- Os router's que são do tipo FFD e que permitem que outros dispositivos se juntem à rede, dando a possibilidade de aumentar o alcance físico. Estes dispositivos não são obrigatórios, apenas são utilizados em caso de necessidade permitindo ainda realizar funções de controlo e monitorização de dispositivos;
- Os *End Devices* podem ser do tipo RFD ou FFD e têm como função realizar o controlo ou monitorizar os dispositivos que se encontram ligados a eles (desde sensores, até controladores).

Numa rede ZigBee com a topologia de estrela existe apenas um dispositivo a funcionar como FFD e os restantes são RFD. Para topologia de tipo ponto a ponto (Peer-to-peer) e em árvore todos os dispositivos devem de ser FFD. Na Figura 3 encontra-se ilustrada as diferentes topologias de redes com a identificação do tipo de dispositivos que esta pode possuir.

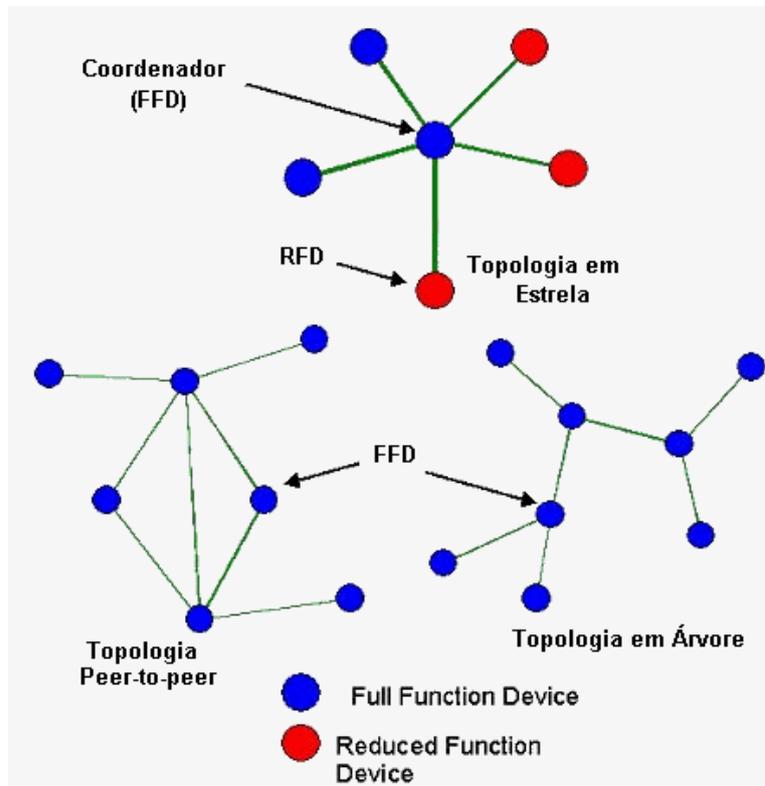


Figura 3 Tipos de dispositivos físicos numa rede ZigBee [13]

O coordenador da rede possibilita ajustar parâmetros de rede, transmitir informações pela rede, gerir os nós da rede, armazenar informações dos nós da rede, distribuir mensagens entre os nós de rede e este normalmente opera no estado ativo.

Os restantes dispositivos da rede têm a função passiva na rede, encontram-se a fazer procura de redes disponíveis, transferem dados da aplicação, determinam o estado dos dados, solicitam dados ao coordenador da rede e podem permanecer durante longos períodos de tempo em modo *sleep*.

### 2.3.2. TOPOLOGIA DA REDE

A norma IEEE 802.15.4 considera três tipos de topologia de rede, a topologia em estrela (*Star*), malha (*Mesh*) e árvore (*Cluster Tree*) [5][8][9].

Em seguida apresenta-se uma representação gráfica e resumida abordagem inerente a cada topologia, podendo cada um deles coexistir dentro de uma rede.

- Topologia em Estrela (*Star Topology*) é composta por um único coordenador que comunica com todos os dispositivos finais (ED) da rede. Estes dispositivos são fisicamente e eletricamente separados uns dos outros onde toda a informação que circula na rede passa pelo nó coordenador. Assim sendo, é o coordenador que inicia a comunicação e mantém os dispositivos a comunicar na rede. Na Figura 4 encontra-se ilustrada uma topologia de rede em estrela com os diferentes dispositivos lógicos possíveis.

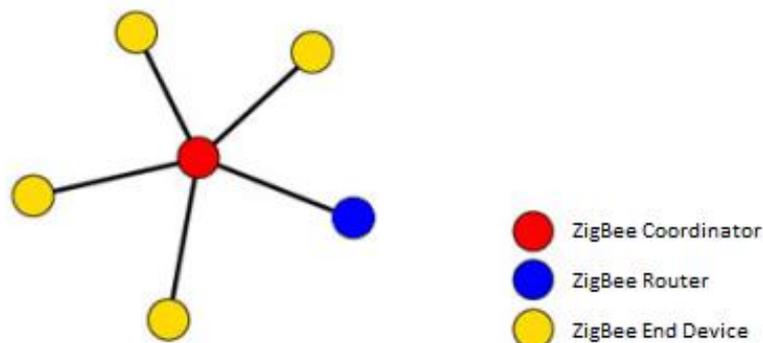
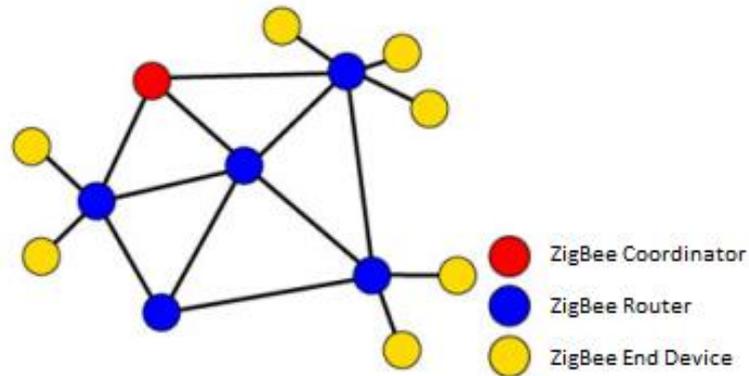


Figura 4 Topologia de rede em Estrela

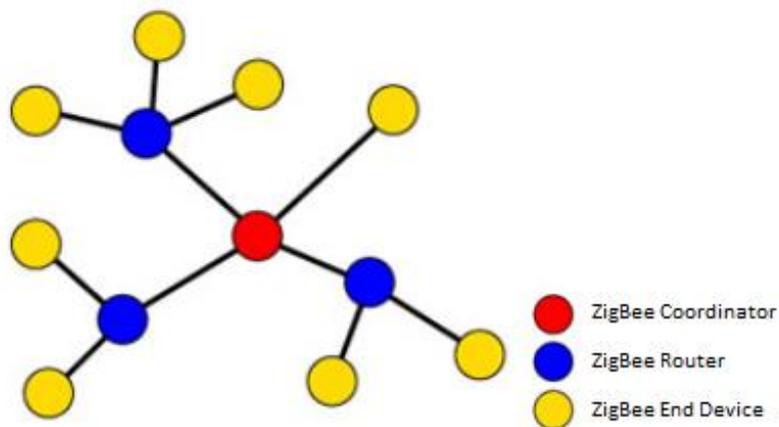
- Topologia em Malha (*Mesh Topology*) permite que os dispositivos podem comunicar com qualquer outro dispositivo dentro do seu alcance. O coordenador regista a

entrada e saída de dispositivos da rede, contudo o fluxo de informação não passa todo pelo coordenador como na topologia estrela, esta topologia permite uma expansão de rede (maior alcance). O modo *beaconing* não é permitido, a sua manutenção é complexa, mas robusta e tolerante a falha. Na Figura 5 encontra-se ilustrada uma topologia de rede em malha com os diferentes dispositivos lógicos possíveis para a comunicação.



**Figura 5 Topologia de rede em Malha**

- Topologia em Árvore (*Cluster Tree Topology*) é similar a topologia em estrela onde a grande diferença é que o nó coordenador pode ter ligação a dispositivos FFD ou RFD, de forma a expandir a rede. Na Figura 6 é ilustrada uma topologia de rede em árvore com as diferentes ligações possíveis aos dispositivos lógicos associados.



**Figura 6 Topologia de rede em Árvore**

### 2.3.3. PROTOCOLOS DE COMUNICAÇÃO ZIGBEE

O protocolo de comunicação definido para a tecnologia ZigBee possui 5 camadas (baseadas no modelo *Open System Interconnection* - OSI), onde as duas camadas mais baixas são definidas pelo IEEE 802.15.4, as duas camadas seguintes são definidas pela *ZigBee Alliance* e a última serão os utilizadores que pretendem criar aplicações.

A pilha protocolar possui as seguintes camadas:

- Camada Física (PHY - *Physical*);
- Camada MAC (*Media Access Control*);
- Camada de Rede (NWK - *Network*) e de Segurança (SSP – *Security Service Provider*);
- Camada de suporte à aplicação;
- Camada de aplicação.

A camada física tem como objetivo realizar a transmissão e a receção de dados através das ondas rádio (por canal físico de rádio frequência), esta camada também possibilita saber qual é a qualidade de conexão, possibilita a deteção de potência dos canais para transmitir através dos melhores nós da rede, e é capaz de verificar quais são os canais ocupados. Esta camada cria uma interface entre a camada MAC e o canal da rádio frequência através do *firmware* e do *hardware* existente.

A camada MAC tem a principal função de controlar o acesso aos canais de rádio frequência, utilizando mecanismos de prevenção de colisão nomeadamente o *Carrier Sense Multiple Access/Collision Avoidance* (CSMA/CA). Para realizar o controlo, este, estabelece uma comunicação com a camada física, além disso especifica o tipo de dispositivos que a rede permite ter, define qual a estrutura de tramas e faz o controlo do processo de sinalização. É nesta camada que se encontra desenvolvido o algoritmo de segurança onde possibilita a confidencialidade, integridade e a autenticidade das tramas [10].

A camada de rede (NWK) define o início ou o fim de um dispositivo ligado à rede e procura dispositivos vizinhos, armazenando informação relativa aos mesmos. Esta camada tem também a função de atribuir os endereços, mas apenas será utilizada pelo coordenador, os

restantes não o farão. Aqui também será realizada a configuração de novos dispositivos e é realizada a descoberta de rotas para fornecer funcionalidades que garantem o correto funcionamento do MAC desta tecnologia e também para fornecer um serviço adequado para fazer a interface com a camada de aplicação.

A camada de suporte à aplicação tal como o nome indica irá ser assegurar uma correta gestão e suporte para as aplicações criadas pelos utilizadores. É esta que fornece uma interface à camada NWK e à camada de aplicação através de um conjunto geral de serviços utilizados pelas aplicações definidas pelo fabricante.

#### **2.3.4. MODOS DE OPERAÇÃO DAS REDES ZIGBEE**

Segundo as referências [8][10][11], numa rede ZigBee, os dispositivos operam em dois modos diferentes:

- No modo *beaconing*, os nós ZigBee *routers* transmitem periodicamente mensagens de sinalização, ou seja, *beacons*, dando informação aos outros nós da sua presença, sendo que os restantes nós só precisam de estar ativos no momento da sinalização. Este modo, permite manter maioria dos dispositivos (*End Devices*) no modo *sleep* entre as sinalizações reduzindo bastante o consumo energético. O modo *sleep* consiste na redução do *duty cycle* dos dispositivos e consequentemente, prolongam a duração bateria a que possam estar ligados.

O intervalo de tempo entre os *beacons* pode variar entre os 15.36 ms e os 251.65 s, para uma taxa de transmissão 250 kbits/s.

Por fim, há que ter em conta o facto de a redução do *duty cycle* (associado a intervalos prolongados entre *beacons*) requer uma temporização de elevada precisão, o que pode colidir com o interesse em produzir um dispositivo de custo reduzido.

- No modo *nom-beaconing* a maioria dos dispositivos mantém os seus recetores permanentemente ativos, havendo um maior consumo energético, podendo tornar necessário fontes de alimentação com maiores capacidades.

A camada MAC é responsável pela programação das transmissões das tramas no modo *nom-beaconing* fazendo uso do método CSMA/CA. Neste método, cada nó

verifica o canal antes de iniciar a transmissão para diminuir a possibilidade de transmissões simultâneas.

Caso o canal esteja livre, o nó inicia a transmissão, caso não esteja livre o nó aborta a transmissão e aguarda um período aleatório para tentar novamente.

## **2.4. TECNOLOGIA BLUETOOTH**

Atualmente o Bluetooth está presente na maior parte dos equipamentos eletrônicos, desde computadores, *smartphones*, *tablets*, automóveis, etc, dando a possibilidade de troca de dados, nomeadamente música, vídeos, fotografias e outros tipos de informação entre dois equipamentos emparelhados.

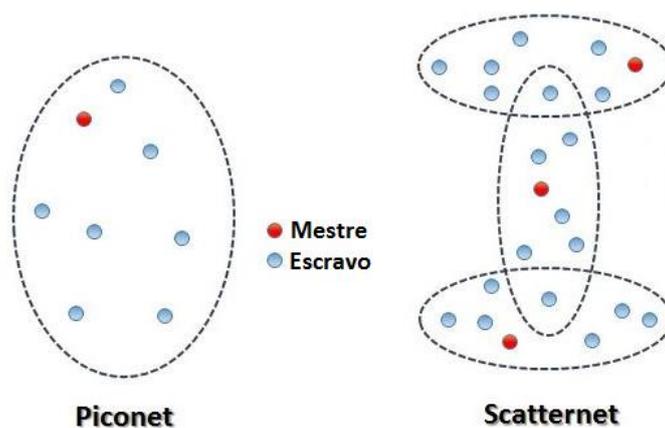
O *Bluetooth* é um protocolo orientado à conexão desenvolvido para permitir a transmissão contínua de dados a uma taxa relativamente elevada, exemplo disso é a sua aplicação nas comunicações de voz. Ao longo do seu desenvolvimento, apesar de existir a preocupação relativa ao consumo energético, o principal foco de desenvolvimento concentrou-se na capacidade de transferência cada vez mais elevada. A vantagem fundamental desta tecnologia é que permite lidar simultaneamente com transmissões de dados e voz, fornecendo aos seus utilizadores variadas soluções.

### **2.4.1. TOPOLOGIA BLUETOOTH**

A conexão dos dispositivos via *Bluetooth* cria uma rede *ad-hoc*, mais conhecida por *piconets*. As *piconets* são estabelecidas dinamicamente e automaticamente sempre que os dispositivos se encontrem ao alcance um do outro, o dispositivo que inicia a conexão assume o papel de *master* (mestre), os restantes dispositivos assumem o papel de *slave* (*escravo*). Uma *piconet* é constituída, no máximo, por oito elementos (um *master* e sete *slaves*) podendo interligar-se entre si ou a dispositivos de outras *piconets*.

Os dispositivos escravos não comunicam diretamente entre si, assim estes dependem do dispositivo mestre para poderem comunicar entre si. Os papéis de mestre e escravo, tem apenas significado numa dada *piconet*, isto porque um dispositivo pode ter ambos papéis se pertencerem a diferente *piconets*. Um dispositivo pode assumir o papel de mestre apenas numa *piconet* mas pode por sua vez ter o papel de escravo noutras *piconetes*.

Uma *scatternet* é um exemplo da interligação entre duas *piconets* diferentes, como se mostra na Figura 7. Essas *piconets* interligadas dentro de uma *scatternet* formam uma infraestrutura para *Mobile Area Network* (MANET) e podem tornar possível a comunicação de dispositivos que não estão diretamente ligados ou que estão fora de alcance.



**Figura 7** Topologias de Rede [16]

Como forma de responder a diferentes necessidades, os dispositivos *Bluetooth* são classificados em três classes, de acordo com o alcance das ondas de rádio dos dispositivos [18], sendo eles:

- Classe 1 – Potência máxima 100mW (20dBm), alcance máximo de 100 metros;
- Classe 2 – Potência máxima 2,5mW (4dBm), alcance máximo de 10 metros;
- Classe 3 – Potência máxima 1mW (0dBm), alcance máximo de 1 metro.

#### **2.4.2. ARQUITETURA**

A arquitetura do *Bluetooth* e as suas características técnicas estão definidas nas especificações denominadas *Core* (núcleo) e *Profiles* (Perfis), definidas pelo SIG (*Special Interest Group*). A especificação do núcleo define como o sistema funciona (protocolos, camadas, especificações técnicas, etc.), enquanto o documento que define os perfis e determina como os diversos elementos que compõem o sistema podem ser empregados para a realização das funções desejadas [19].

A arquitetura do *Bluetooth* está dividida em dois componentes: um *transceiver* (hardware) e uma pilha de protocolos (software), esta arquitetura oferece serviços e funcionalidades básicas que possibilitam a conexão e troca de dados entre dispositivos.

A tecnologia Bluetooth opera na faixa de rádio não licenciada ISM (Industrial, Scientific, Medical) entre 2.4 GHz e 2.485 GHz, o sistema utiliza um mecanismo designado *frequency hopping*, que “salta” constantemente de frequência para evitar a interferência e enfraquecimento do sinal, a cada segundo são realizados 1600 saltos de frequência.

#### 2.4.2.1. PILHA DE PROTOCOLOS

A pilha de protocolos na especificação *Bluetooth* é dividida em três grupos lógicos: Grupo de protocolos de transporte, Grupo de protocolos de *middleware* e o grupo de aplicação [17][18][19], como ilustrado na Figura 8.

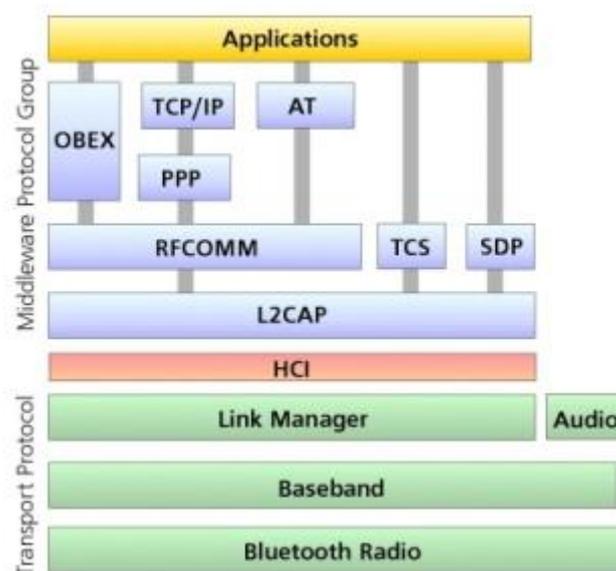


Figura 8 Pilha de Protocolos [17]

O grupo de protocolos de transporte permite um dispositivo localizar outro dispositivo e gerir *links* físicos e lógicos das camadas superiores, estes protocolos correspondem às camadas físicas e de enlace do modelo OSI. As camadas de rádio frequência (RF – *Radio Frequency*), *Baseband*, *Link Manager*, *Logical Link Control and Adaptation* (L2CAP) fazem parte dos protocolos de transporte. Estes protocolos permitem comunicações síncronas e assíncronas.

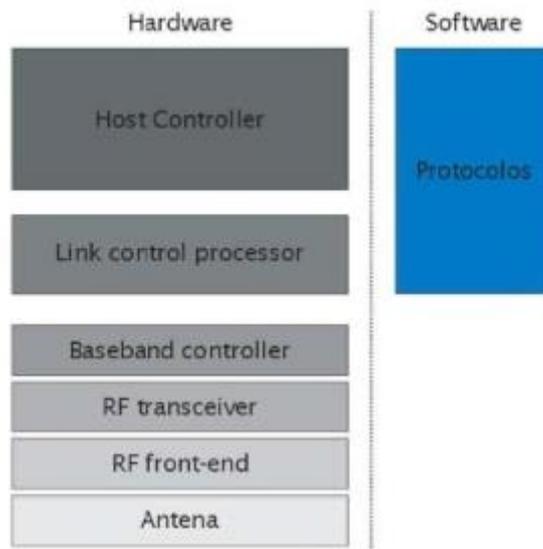
O grupo de protocolos de *middleware* inclui protocolos de terceiros e *standards industriais*. Estes protocolos fazem uma forma de “tradução” que permite a operacionalidade de novas aplicações ou aplicações já existentes. Protocolos *standards* industriais incluem *Point-to-Point Protocol* (PPP), *Internet Protocol* (IP), *Transmission Control Protocol* (TCP) *Wireless Application Protocol* (WAP), etc. Outros protocolos desenvolvidos pelo próprio SIG também foram incluídos.

O grupo de aplicação consiste das próprias aplicações que utilizam *links Bluetooth*.

#### **2.4.2.2. HARDWARE BLUETOOTH**

Os dispositivos que implementam especificações *Bluetooth* devem possuir seis componentes de *hardware* [17][18][19], como mostra a Figura 9. Os elementos de *hardware* são:

- *Host Controller*: Elemento de *hardware* responsável pelo processamento de código de alto nível de aplicações e de algumas camadas inferiores;
- *Link Control Processor*: Elemento responsável pelo processamento das camadas mais baixas do protocolo como *Link Manager* e *Link Controller*;
- *Baseband Controller*: Elemento lógico responsável pelo controlo do *transceiver* de rádio frequência (RF);
- *Transceiver RF*: Elemento que contém o filtro passa banda da antena, amplificador de ruídos e amplificador de energia. Responsável pela troca de dados entre o emissor e o recetor.
- Antena: Este elemento pode ser interno integrado em componentes de terceiros ou externo.



**Figura 9 Hardware Bluetooth [17]**

### 2.4.3. ESTADO DA CONEXÃO BLUETOOTH

O dispositivo *Bluetooth* dependendo das operações exercidas pode estar em dois estados principais, onde cada estado é caracterizado por um consumo de energia diferente, sendo eles:

- *Standby*: Este é o estado pré-definido. Neste estado os dispositivos estão prontos para iniciar a conexão, trata-se de um estado de baixo consumo de energia em que apenas o relógio interno do dispositivo está em execução;
- *Connection*: Este estado indica que o dispositivo está a trocar dados com outro dispositivo.

Na transição entre os estados principais apresentados, existem outros estados de transição, na Figura 10 está apresentado o diagrama de estados das conexões *Bluetooth* [19].

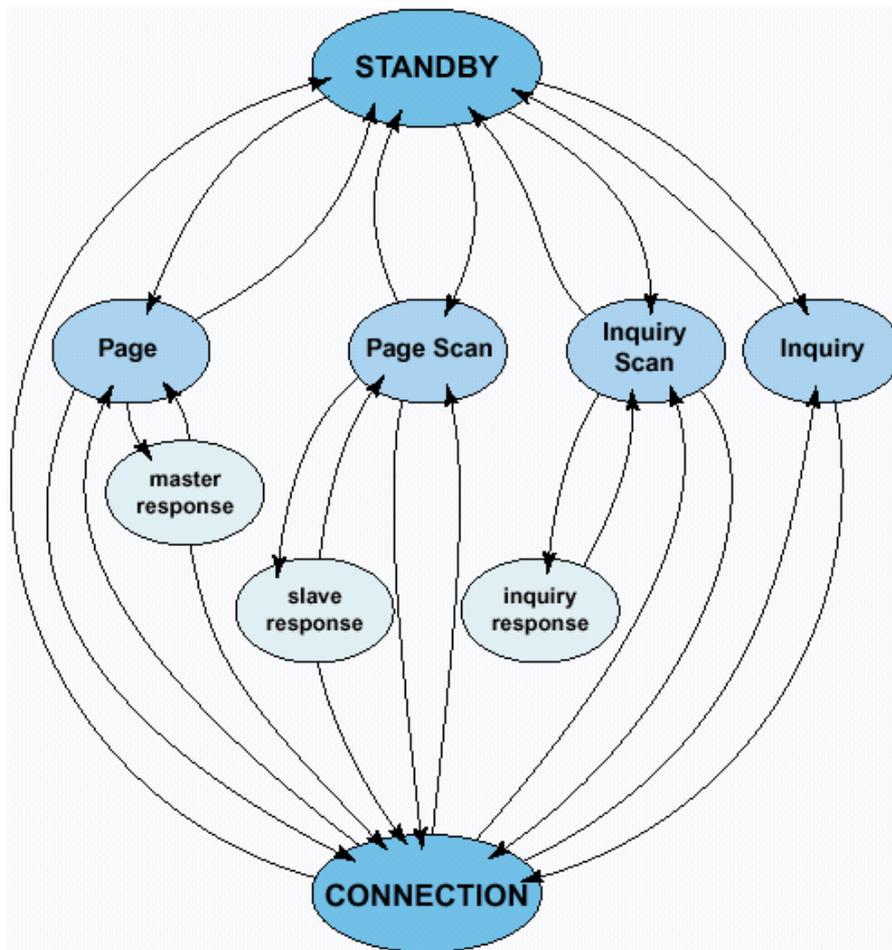


Figura 10 Diagrama de Estados [19]

#### 2.4.3.1. ESTABELECIMENTO DE CONEXÃO

O estabelecimento de conexão é realizado através dos procedimentos de *inquiry* e de *paging*. Com o procedimento de *inquiry* é possível detetar qual os dispositivos que estão ao alcance do dispositivo fonte. Este procedimento tem início quando o dispositivo fonte entra no estado *inquiry*, no qual difunde pela rede pacotes *inquiry* (pacotes do tipo ID). Estes pacotes são enviados seguindo uma sequência de frequências designada *inquiry hopping sequence*.

Para responder a este pacote, o dispositivo destino deve encontrar-se no estado *inquiry scan*, ao receber o pacote de *inquiry*, ele passa para o estado de *inquiry response*, no qual um pacote de resposta (pacote FHS (*Frequency Hopping-Synchronization*)). Este pacote é enviado utilizando uma sequência denominada *inquiry response hopping sequence*.

Após este procedimento, é realizado o procedimento de *paging*, que resulta no estabelecimento de uma conexão entre o *master* e o *slave*. O dispositivo fonte passa a ser o *master* da conexão [19].

Quando um dispositivo está no estado de conexão, este pode encontrar-se em diferentes modos de operação [19]:

- Modo Ativo: neste modo o dispositivo participa ativamente no canal, pode ser também designado estado de transmissão;
- Modo *Sniff*: trata-se de um modo de baixo consumo, o dispositivo *slave* escuta a rede em intervalos fixos, sendo dependente da aplicação;
- Modo *Hold*: este modo também é de baixo consumo, o dispositivo fica inativo durante um certo período de tempo, sem qualquer transmissão de dados. Após esse período o aparelho reinicia as transmissões;
- Modo *Park*: modo de menor consumo de energia. Neste modo o dispositivo ganha um endereço referente ao modo *Park*, ainda pertencendo à rede. A diferença é que assim não participa na transmissão de dados.

## 2.5. TECNOLOGIA NFC – NEAR FIELD COMMUNICATION

O NFC é uma tecnologia emergente focada nas comunicações *contactless*. Esta tecnologia evolui da combinação da tecnologia RFID e *Smart Card*, sendo compatível com as aplicações RFID. A principal diferença é que a tecnologia RFID comunica a distâncias maiores enquanto a tecnologia NFC permite a partilha de informação entre dois dispositivos a uma distância inferior a 4 cm.

A identificação por rádio frequência tem origem no funcionamento dos sistemas de radares. Este princípio de identificação foi inventado em 1935 pelo físico Escocês *Robert Alexander Watson-Watt* e utilizado na segunda guerra mundial para alertar com antecedência a presença de aviões quando ainda estavam distantes. A Inglaterra, tendo *Watson-Watt* do seu lado, desenvolveu o primeiro identificador designado IFF (*Identify Friend or Foe*). Todos os aviões britânicos receberam um transmissor que ao receber sinais das estações de radar, começavam a transmitir um sinal de resposta. Os RFID atuais usam o mesmo princípio de funcionamento, um sinal é enviado a uma tag, esta reflete de volta o sinal (sistema passivo)

ou transmite o seu próprio sinal (sistema ativo). A primeira utilização comercial do RFID foi implementada nos sistemas anti-roubo, que utilizam ondas de rádio para determinar se um produto tinha sido roubado ou pago. Foi nesse contexto que surgiram as *tags*, que fazem parte do sistema de RFID até hoje [20].

Esta tecnologia de curto alcance opera na frequência 13,56 MHz, com uma velocidade máxima de comunicação de 424 kbps, onde a comunicação é iniciada quando se aproxima dois dispositivos NFC, como o alcance de transmissão de informação é curto, as transações NFC são intrinsecamente seguras, pois dificulta a interceção do sinal por outros dispositivos.

A tecnologia NFC harmoniza diversas tecnologias sem contato atualmente, permitindo soluções em áreas como a recolha/troca de informação, controlo de acesso, cuidados de saúde, transportes, pagamentos, acesso a informação através de um cartaz inteligente, entre outros [22].

### 2.5.1. PRINCÍPIO DE FUNCIONAMENTO

A principal característica do NFC é a interface de comunicação sem fio com uma distância de trabalho limitada a cerca de 10 cm. A interface pode funcionar em vários modos. Os modos são distinguidos se um dispositivo cria o seu próprio campo, designa-se por dispositivo ativo, caso contrário designa-se por passivo. Os dispositivos ativos normalmente têm uma fonte de alimentação, enquanto os dispositivos passivos geralmente não (*Smart Card*). O acoplamento indutivo leva os dispositivos passivos a absorver energia do dispositivo ativo quando estes ficam suficientemente próximos. Uma vez ligado, o dispositivo passivo pode comunicar e trocar dados com outro dispositivo. Quando dois dispositivos comunicam, existem três configurações possíveis. Estas são descritas na Tabela 2 [24].

**Tabela 2 Configurações da comunicação [24]**

<b>Dispositivo A</b>	<b>Dispositivo B</b>	<b>Descrição</b>
<b>Ativo</b>	<b>Ativo</b>	Quando um dispositivo envia dados, cria um campo RF. Quando um dispositivo está á espera de dados não gera nenhum campo RF. Deste modo, o campo RF é alternadamente gerado pelo dispositivo A e B.
<b>Ativo</b>	<b>Passivo</b>	O campo RF é gerado apenas pelo Dispositivo A.
<b>Passivo</b>	<b>Ativo</b>	O campo RF é gerado apenas pelo Dispositivo B.

Estas configurações são importantes porque a forma como os dados são transmitidos depende de o dispositivo estar a transmitir em modo ativo ou modo passivo.

Adicionalmente ao modo ativo e passivo existem dois papéis diferentes que um dispositivo pode desempenhar numa comunicação NFC. O NFC baseia-se no conceito de mensagem resposta. O que significa que um dispositivo A envia uma mensagem para outro dispositivo B, que devolve de seguida uma resposta ao dispositivo A. Não é possível ao dispositivo B enviar quaisquer dados para o dispositivo A sem primeiro receber alguma mensagem do dispositivo A, para então poder responder. O papel do dispositivo A, que inicia a troca de dados, é de iniciador, o papel do outro dispositivo é de destino. A Tabela 3 lista todas as combinações possíveis destes papéis no que respeita ao modo passivo e ativo [24].

**Tabela 3 Combinação dos modos Ativo/Passivo como Iniciador/Destino [24]**

	<b>Iniciador</b>	<b>Destino</b>
<b>Ativo</b>	Possível	Possível
<b>Passivo</b>	Não é possível	Possível

Além disso a comunicação NFC não está limitada a um par de dispositivos. Na verdade, um dispositivo iniciador pode comunicar com múltiplos dispositivos destino, mas não em simultâneo. Neste caso todos os dispositivos destinos são ativos ao mesmo tempo, mas antes de enviar a mensagem, o dispositivo iniciador seleciona o dispositivo destino, e os restantes que não foram selecionados devem ignorar a mensagem enviada. Apenas o dispositivo destino selecionado pode responder aos dados recebidos [24].

### **2.5.2. NORMAS E ESPECIFICAÇÕES NFC**

O NFC é baseado em normas reconhecidas de forma a desbloquear todos os recursos da tecnologia [21][22], assim sendo são apresentadas as duas normas principais:

- ISO/IEC 18092, “*Near Field Communication – Interface Protocol*” (NFCIP - 1), foi aprovada em 2003 e recentemente revista em 2013. A norma especifica a interface e o protocolo para comunicações simples sem fio entre dispositivos próximos, tendo como objetivo garantir a interoperabilidade entre dispositivos NFC de diferentes fabricantes. A ISO/IEC 18092 tem como base normas existentes, RFID, ISO/IEC 14443 e JIS 6319-4 que também operam na frequência de 13,56 MHz. Isto permitiu que os dispositivos NFC fossem compatíveis com outras implementações “*Smart*

*Card*” incluindo os sistemas FeliCa da Sony e MIFARE da NXP Semicondutores. Uma norma idêntica foi aprovada pela ECMA *International*, ECMA – 340.

- ISO/IEC 21481, “*Near Field Communication – Interface Protocol - 2*” (NFCIP - 2), foi aprovada pela primeira vez em 2005 e mais recentemente revista em 2012. Esta norma determina qual dos três protocolos *standard*, ISO/IEC 18092, ISO/IEC 14443 ou ISO/IEC 21481, será usado para a troca de dados específicos. A inclusão da ISO/IEC 15693 é destinada a melhorar a interoperabilidade entre as tecnologias NFC e RFID. Outra norma idêntica foi aprovada pela ECMA *International*, ECMA – 352.

As especificações e as normas relacionadas com o NFC são desenvolvidas e mantidas pela organização sem fins lucrativos *NFC Forum*, fundada em 2004 pela Sony, Philips e Nokia, até a data o fórum lançou 18 especificações, entre elas estão os tipos de tags, que será abordado como mais detalhe no ponto 2.5.4, o *NFC Data Exchange Format* (NDEF) que especifica o formato de mensagem em que os dados podem ser armazenados na tag NFC e/ou transmitidos entre dispositivos compatíveis com o NFC. O *NFC Record Type Definition* (RTD) descrevem o tipo de registos comuns, foram criados RTDs específicos para cadeias de texto, cartazes inteligentes, *Uniform Resource Identifiers* (URIs) e assinaturas digitais. O *NFC Controller Interface* (NCI) normaliza as interações entre um dispositivo NFC e o chip controlador de NFC que detém. O NCI torna mais fácil para os fabricantes de dispositivos integrar *chipsets* de fabricantes de *chips* diferentes, e define um nível de funcionalidade e interoperabilidade entre os componentes dentro de um dispositivo NFC comum. O *NFC Logic Link Control Protocol* (LLCP) define um protocolo da camada dois do modelo OSI para suportar as comunicações *peer-to-peer*. Esta especificação define dois tipos de serviço, sem conexão e orientado por conexão, organizado em três classes de serviço de ligação: serviço sem conexão única; serviço orientado a conexão única; e ambos sem conexão e serviço orientado. O serviço sem conexão oferece uma configuração mínima sem garantia de segurança ou controlo de fluxo. O serviço orientado a conexão oferece uma entrega segura, controlo de fluxo e multiplexação de camadas de serviço baseada em sessão. Este protocolo é baseado na norma IEEE 802.2, definido para suportar aplicações com dados limitados.

As especificações mais recentes abordam casos de uso específico de NFC. Dispositivos pessoais de saúde, monitores cardíacos, Pedômetros entre outros [21][22].

### 2.5.3. MODOS DE OPERAÇÃO

Segundo o NFC *Forum* [21][23], existem três modos de operação distintos, cada dispositivo NFC podem alterar o seu modo de operação de acordo com a sua necessidade, isto torna os dispositivos mais interessantes, na Figura 11 aparece ilustrado os diferentes modos de operação.



Figura 11 Modos de Operação NFC [22]

- Modo *Read/Write* – Permite aos dispositivos com tecnologia NFC ler e escrever em qualquer um dos tipos diferentes de tags especificadas pelo NFC Fórum, como ler uma tag NFC de um cartaz inteligente. No modo *Read/Write* há compatibilidade da interface RF com a norma ISSO 14443 e Felica.
- Modo *Peer-to-Peer* – Permite que dois dispositivos NFC troquem dados entre si, como por exemplo a troca de fotografias ou cartões de visita digitais entre telemóveis. Este modo é normalizado no *standard ISO/IEC 18092*.
- Modo *Card Emulation* – Neste modo o dispositivo NFC comporta-se como *Smart Card* tradicional, por exemplo cartão de crédito e débito, permitindo o pagamento sem contato e emissão de bilhetes por meio do dispositivo NFC sem necessidade de mudar a infraestrutura existente.

Os três modos apresentados têm importantes diferenças técnicas, na prática, estes são indiferenciados e principalmente indistinguíveis para o utilizador final.

#### 2.5.4. TAGS NFC

As tags NFC são um pequeno circuito impresso, semelhante a tag RFID. De forma a garantir a operação entre diferentes tecnologias. O objetivo destas especificações é definir como as mensagens NDEF são lidas e gravadas em tags NFC. Segundo o NFC Forum existem quatro tipos de tags [21][22], assim sendo são apresentados os diferentes tipos e as suas especificações:

- TAG TYPE1: baseada na ISO/IEC 14443A, operam a 106 Kbps e podem armazenar 96 bytes, embora possa ser expandido até 2 Kbyte. Esta tag é fabricada como regravável, mas pode ser bloqueada pelo utilizador e tornar-se apenas de leitura;
- TAG TYPE 2: baseada na ISO/IEC 14443A, operam a 106 Kbps e podem armazenar 48 bytes, embora pode ser também expandido para armazenar até 2 Kbyte. Semelhante a tag Type1, esta também são regraváveis, mas podem ser bloqueadas apenas para leitura;
- TAG TYPE 3: baseada na JIS 6319-4, também designada FeliCa, opera em 212 Kbps e podem armazenar até 1 Mb. Esta tag é definida como regravável ou apenas de leitura no seu fabrico.
- TAG TYPE 4: totalmente compatível com a ISO/IEC 14443, opera em 424 Kbps e pode armazenar até 32 Kbytes. Esta tag também é pré-configurada no momento de fabrico se é regravável ou apenas de leitura. A interface de comunicação é compatível com a ISO/IEC 14443 A/B.

Todas as tags são elementos passivos e não precisam de fonte de alimentação. As tags NFC são semelhantes aos códigos QRCode, na medida em que são *user-friendly* [22].

#### 2.6. TECNOLOGIA ETHERNET

O primeiro sistema “Ethernet” foi desenvolvido pela Xerox Parc em 1972, o primeiro sistema experimental foi designado “Alto Aloha Network”, em 1973 este sistema mudou de nome para “Ethernet”. A primeira norma foi desenvolvida por um conjunto de empresas designado DIX, *Digital Equipment Corporation* (DEC), Intel e Xerox, a norma Ethernet 10 Mb/s.

A Ethernet é uma tecnologia de redes área local (LAN – *Local Area Network*), no qual tem uma área geográfica relativamente pequena, normalmente definida dentro de um edifício. Uma LAN é um conjunto de computadores conectados entre si numa área local para comunicarem entre si. Os dados são enviados na forma de pacote, para controlar a transmissão dos pacotes, podem ser usadas diferentes tecnologias [25].

### **2.6.1. NORMAS ETHERNET**

A primeira norma da tecnologia Ethernet foi a DIX, como já referida anteriormente, esta norma foi revista para adicionar melhorias surgindo assim a DIX v2.0. Em paralelo com estas melhorias, O IEEE também estava a desenvolver uma norma. Consequentemente, a tecnologia Ethernet original, baseada na utilização de um cabo coaxial grosso para fornecer um canal de comunicação partilhado, acabou por ser normalizado duas vezes, pelo consórcio DIX e pelo IEEE [25].

A Ethernet pertence á família de produtos LAN, definidos pela norma IEEE 802.3, que define o protocolo CSMA/CD – *Carrier Sense Multiple Access with Collision Detect*. Atualmente são definidos quatro taxas de transmissão de dados para operação em cabo de par trançado e fibra ótica: 10Base-T Ethernet (10 Mb/s), *Fast Ethernet* (100 Mb/s), *Gigabit Ethernet* (1000 Mb/s) e 10-Gigabit Ethernet (10 Gb/s) [27].

A norma IEEE é atualmente mantida pela norma IEEE 802 LAN/MAN (*Metropolitan Area Network*).

As redes Ethernet utilizam o protocolo CSMA/CD para coordenar o acesso ao meio de transmissão. O endereçamento é feito com base numa sequência de 6 bytes (48 bits) habitualmente conhecida por endereço físico, endereço MAC ou endereço “Ethernet”.

### **2.6.2. SISTEMA ETHERNET**

Uma rede Ethernet é composta por hardware e software, trabalham em conjunto para fornecer dados digitais entre computadores. Para realizar essa tarefa, vários elementos básicos operam para fazer um sistema Ethernet [25].

#### **2.6.2.1. ELEMENTOS BÁSICOS**

O sistema Ethernet é composto por quatro blocos fundamentais, serão descritos de seguida [25]:

- *Frame* Ethernet – conjunto normalizado de bits usados para transportar dados sobre o sistema;
- Protocolo MAC – consiste num conjunto de regra incorporado em cada interface Ethernet que permite estações Ethernet aceder ao canal Ethernet em modo *half-duplex* ou *full-duplex*;
- Componentes de Sinalização – dispositivos eletrónicos normalizados que enviam e recebem sinais através de um canal de Ethernet;
- Meio físico – cabos e outros equipamentos usados para transportar sinais digitais entre os computadores ligados à rede.

### 2.6.2.2. FRAME ETHERNET

A organização da *frame* Ethernet é fundamental para o funcionamento do sistema. A primeira *frame* foi definida pela DIX, mais tarde foi modificada pela norma IEEE 802.3. A norma DIX definiu um campo designado “*type*”, a primeira norma 802.3 especifica este campo como um campo de comprimento, com um mecanismo que permitiu que ambas as versões coexistissem no mesmo sistema Ethernet. A Figura 12 mostra as versões da *frame* Ethernet DIX e IEEE [25].

Ethernet II DIX Frame							
64 bits	48 bits			48 bits	16 bits	368 to 12000 bits (46 to 1500 bytes)	32 bits
Preamble	Individual/ Group Address Bit	Destination Address		Source Address	Type	Data	Frame Check Sequence

IEEE 802.3 Frame								
56 bits	8 bits	48 bits			48 bits	16 bits	368 to 12000 bits (46 to 1500 bytes)	32 bits
Preamble	SFD	Individual/ Group Address Bit	Globally/ Locally Administered Address Bit	Destination Address	Source Address	Length	LLC/Data	Frame Check Sequence

Figura 12 Versões de Frame [26]



# 3. ARQUITETURA GERAL

Ao longo dos capítulos 1 e 2 foram apresentadas algumas tecnologias necessária para realizar o controlo do quarto de hotel. Deste modo, nesta secção será feito um enquadramento geral do projeto *Smart Hotel*, assim como, a apresentação da arquitetura geral do mesmo. Será também abordado o projecto do presente relatório, onde estará descrito os módulos necessários para cumprir com os requisitos.

## 3.1. ENQUADRAMENTO PROJETO *SMART HOTEL*

O projeto consiste num sistema tecnologicamente inovador para os hotéis modernos, fazendo uso das tecnologias/ferramentas mais utilizadas hoje em dia, nomeadamente a internet e os equipamentos móveis, desta forma pretende-se tornar os processos *check-in* e *check-out* mais rápido e automático. Através das novas tecnologias pretende-se dar resposta ao cliente e ao mercado cada vez mais exigente.

A solução disponibiliza um *website* do hotel, no qual o cliente pode aceder com recurso a um *smartphone* com ligação a internet onde poderá consultar informação dos quartos que hotel dispõe e a sua topologia, pode também fazer simulações de reserva, assim como, fazer as reservas pretendidas. No *website* o cliente pode após efetuar a reserva, fazer o seu registo com a informação necessária e obrigatória, aqui pode também deixar previamente a informação importante para o conforto da sua estadia, ou seja, informação de possíveis restrições alimentares por motivos de saúde, pedidos de serviços, por exemplo, cama extra para crianças, entre outra informação que for necessária para o cliente.

O sistema de gestão do hotel recebe alertas das reservas e toda a informação registada pelo cliente, podendo antecipadamente os recursos do hotel fazerem a preparação para receberem o cliente, permitindo desta forma aumentar a qualidade e o nível do serviço dos hotéis.

O cliente quando chega ao hotel, faz o check-in na receção do hotel, onde deverá fazer o registo do seu *smartphone* que será usado como chave do quarto, dessa forma completar a validar a informação da sua reserva.

Dentro do hotel o cliente pode conectar-se a rede do hotel e instalar no seu *smartphone* a aplicação mobile, esta aplicação disponibiliza todo o material de comunicação do hotel e também um painel de controlo para o controlar os dispositivos no interior do quarto, ou seja, iluminação, ar condicionado, televisão, estores, entre outros. O *smartphone* para fazer o controlo dos dispositivos deve estar conectado à central do quarto por Bluetooth, assim o cliente pode predefinir a temperatura e iluminação desejada.

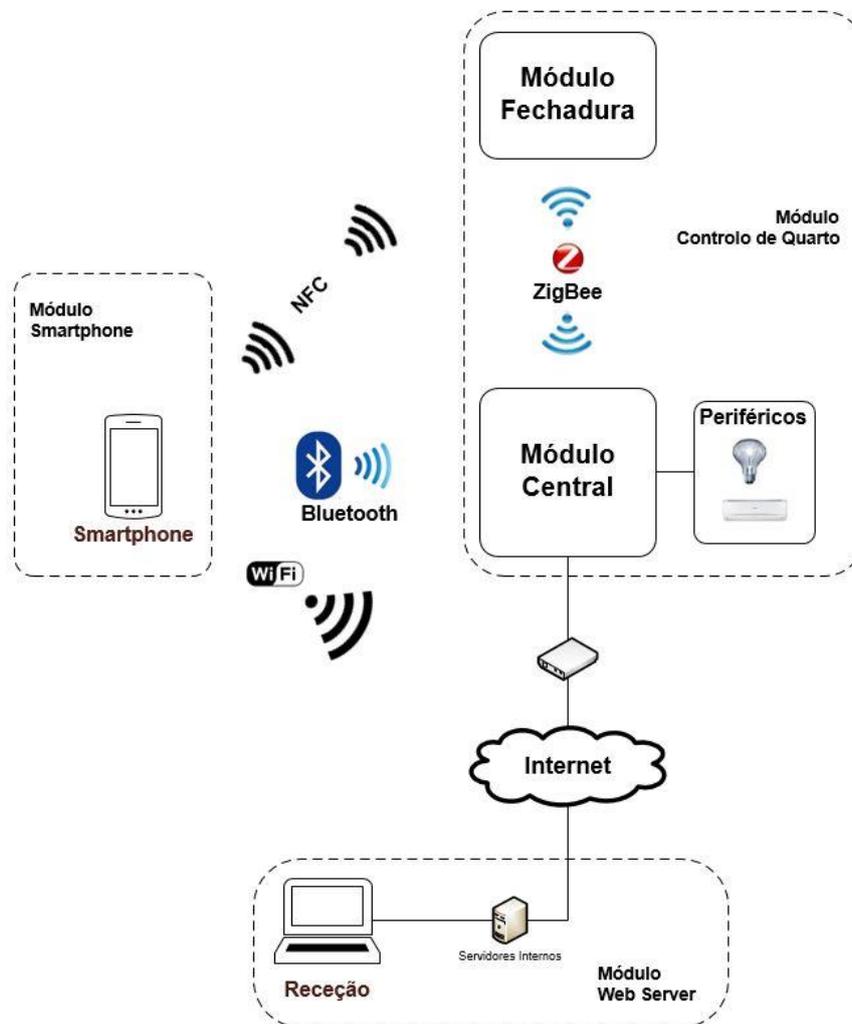
Para entrar no quarto do hotel, o cliente aproxima o *smartphone* do leitor da porta do quarto e sendo a porta correta esta irá abrir, subcapítulo 3.4, será abordado e explicado com mais detalhe todo o controlo de acesso do quarto assim o controlo dos dispositivos no interior do quarto.

### **3.2. ARQUITETURA GERAL DO PROJETO *SMART HOTEL***

Devido a dimensão do projeto, este foi dividido em três módulos. Estes serão desenvolvidos por três alunos do ISEP, o módulo *Web Server* é o desenvolvimento de um *website* e a sua interligação ao sistema de gestão do hotel, assim como também as interligações da rede do hotel aos quartos e aos equipamentos móveis. O módulo *Smartphone* trata-se de uma aplicação mobile para o hotel, esta aplicação como já mencionado anteriormente, faz a interface com a central do quarto para o controlo dos periféricos no interior do quarto. Por último módulo Controlo de Quarto é o desenvolvimento do sistema de controlo de quarto de hotel, que implica o controlo de acesso ao quarto e o controlo efetivo dos periféricos presentes no quarto, sendo este o âmbito de desenvolvimento do presente relatório.

A Figura 13 apresenta a arquitetura geral do projeto *Smart hotel*, onde estão representados os três módulos e as interligações entre si, assim como, as respetivas comunicações envolvidas. O foco deste relatório é o desenvolvimento do sistema de controlo do quarto do

hotel, este comunica com os restantes subprojectos por Bluetooth com a aplicação *mobile* do *Smartphone* e por *Ethernet* ao sistema de gestão do hotel.



**Figura 13 Arquitetura Geral – Smart Hotel**

Na Figura 13, o sistema de controlo do quarto está representado por dois módulos principais, o módulo da fechadura e o módulo central. O *smartphone* comunica com o módulo da fechadura por comunicação NFC, este por sua vez, comunica com o módulo central por comunicação ZigBee. Seguidamente será abordado com mais detalhe a estrutura dos dois módulos referidos.

### **3.3. REQUISITOS DO SISTEMA MÓDULO CONTROLO DO QUARTO**

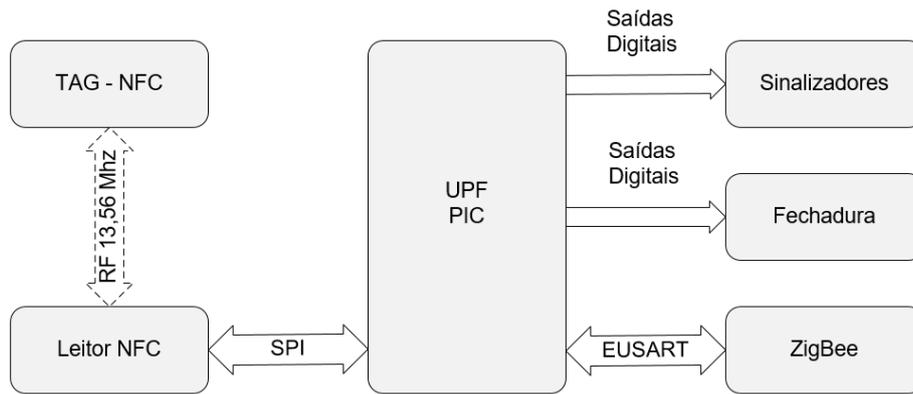
De forma a dar resposta à arquitetura apresentada do sistema, será apresentado de seguida alguns dos requisitos capazes de justificar as opções tomadas ao longo do desenvolvimento do trabalho relativas ao módulo controlo do quarto, sendo eles:

- Controlo de acesso ao quarto através do *smartphone*;
- Comunicação Bluetooth com *smartphone*;
- Controlo de periféricos (Iluminação, TV, A/C, Estores) pelo *smartphone*;
- Estabelecer comunicação entre o módulo central e o *Web Server*.

### **3.4. ARQUITETURA MÓDULO FECHADURA**

A Figura 14 apresenta a arquitetura do módulo da fechadura, onde estão representados os blocos necessários para o seu funcionamento, bem como respetivas interligações e comunicações existentes entre si. O módulo desenvolvido é o sistema elétrico da fechadura da porta do quarto do hotel, sendo responsável pelo controlo da mesma.

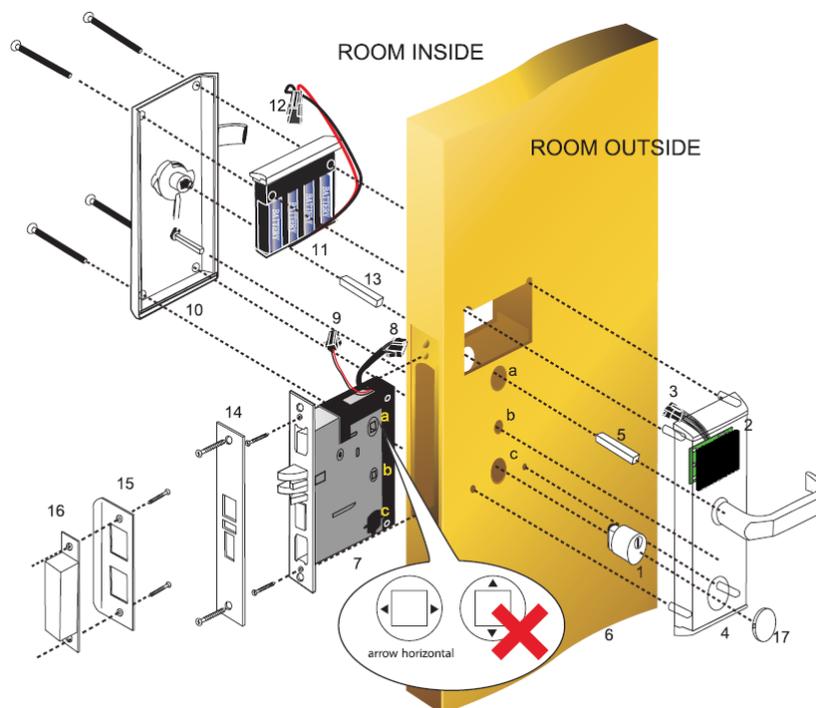
O bloco central deste módulo é a Unidade de Processador da Fechadura (UPF), como o nome indica, trata-se do processador do módulo, este comunica com dois blocos essenciais, o leitor de NFC e o ZigBee. O leitor NFC é responsável pela leitura da tag NFC do *smartphone* que estiver na proximidade do leitor da porta, a leitura efetuada é processada pela UPF e enviada de seguida para o módulo central através do ZigBee. O resultado desta comunicação irá permitir ou não a abertura da porta, caso seja recebido a informação de abertura, a UPF aciona a fechadura e em simultâneo a sinalização respetiva para o efeito (sinalizador luminoso verde).



**Figura 14 Arquitetura Módulo Fechadura**

A fechadura trata-se de uma fechadura eletrônica que atualmente já existem nos hotéis, contudo as fechaduras presentes na maioria dos hotéis são de leitores de cartões RFID, na Figura 15 está ilustrado a estrutura de uma fechadura, este projeto pretende utilizar essas fechaduras, contudo o leitor (2) é um leitor NFC.

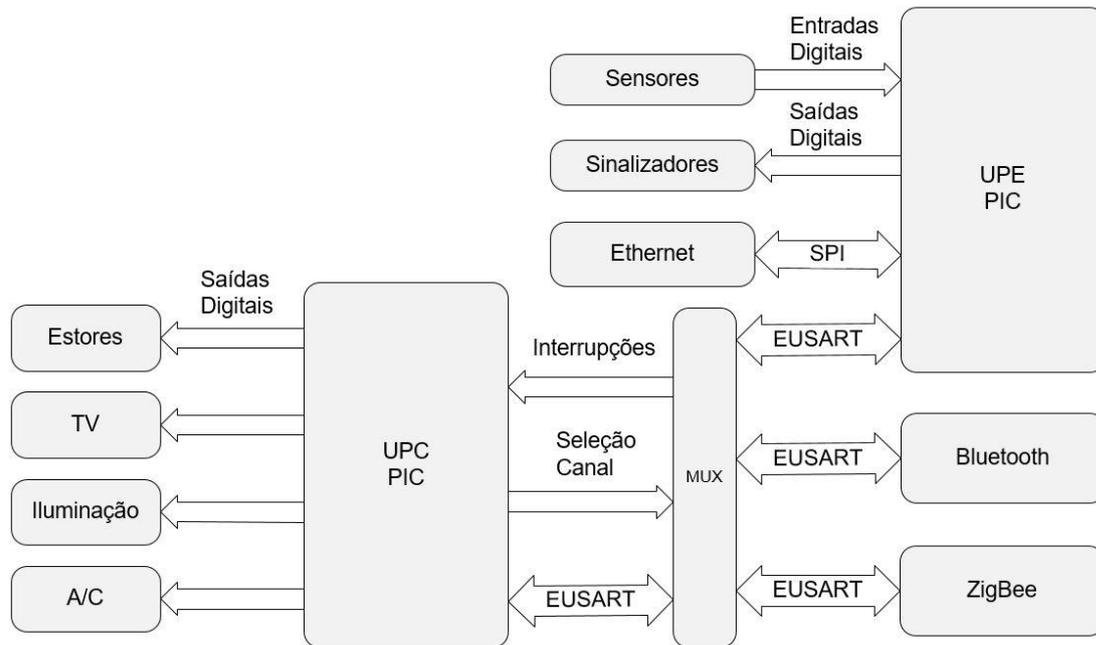
A evolução das fechaduras nos hotéis passa pela incorporação do leitor e painel da fechadura na própria estrutura da porta, onde menos é mais, isto permite adaptar em qualquer porta independentemente do seu *design*.



**Figura 15 Montagem de Fechadura**

### 3.5. ARQUITETURA MÓDULO CENTRAL

A Figura 16 apresenta a arquitetura do módulo e os seus vários blocos. Este módulo possui dois blocos principais que garantem o seu correto desempenho, a Unidade de Processador Central UPC e a Unidade de Processador da Ethernet (UPE). A utilização de duas unidades de processamento deve-se principalmente aos blocos de comunicação necessários para responder aos objetivos do projeto. Este módulo fica instalado no quadro elétrico do quarto.



**Figura 16 Arquitetura Módulo Central**

A UPE está dedicada à comunicação Ethernet, devido à complexidade desta comunicação, este processador dispõe também de sinalizadores, permitindo indicar facilmente alguns status de funcionamento do processador. O processador também faz a leitura de dois sensores do interior do quarto.

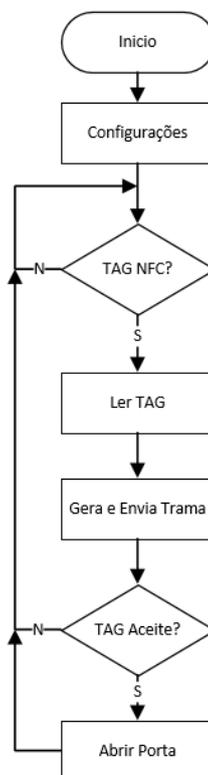
A UPC é responsável pela gestão dos blocos de comunicação existentes no módulo, para isso, este processador controla um multiplexador (MUX) que estabelece a ligação com os diversos blocos que deve estar a comunicar em cada instante. O MUX permite comutar entre os blocos de comunicação garantido o funcionamento de todos os blocos, a UPE é um dos blocos que comunica com a UPC através do MUX, assim como, o Bluetooth e o ZigBee. O Bluetooth comunica com a aplicação do *smartphone* para o controlo dos periféricos do quarto, o ZigBee comunica com o módulo da fechadura para permitir ou não a abertura da porta do quarto.

A UPC é também responsável pelo acionamento dos periféricos do quarto, tais como, Estores, Iluminação, TV e A/C, de acordo com a informação recebido pelo *Bluetooth*.

A localização deste módulo facilita a interligação com os atuadores elétricos dos periféricos mencionados, assim como, a sua alimentação.

### 3.6. ARQUITETURA DE SOFTWARE

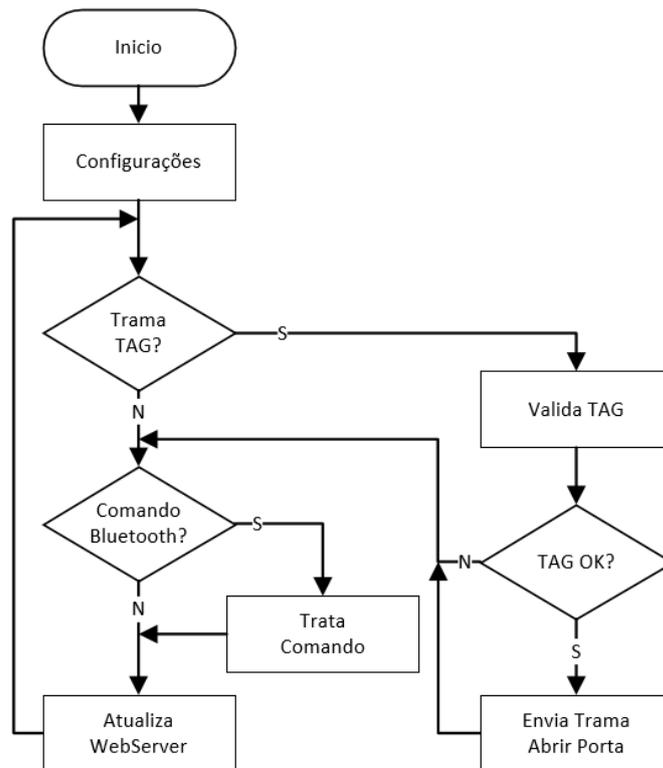
Em termos funcionais foram desenvolvidas aplicações específicas para cada um dos módulos utilizados. Uma vez que os dois módulos são controlados através de microcontroladores, de seguida será apresentado um fluxograma para melhor compreensão do seu funcionamento.



**Figura 17** Arquitetura *Software* Módulo Fechadura

A Figura 17 descreve o algoritmo desenvolvido para o módulo da fechadura, ele irá controlar a fechadura da porta do quarto de hotel. O módulo irá iniciar e realizar as suas configurações iniciais, de seguida o sistema aguarda até detetar uma tag NFC. Após a deteção de uma tag é feita a sua leitura, de seguida a construção da trama e o envio para o módulo central que vai fazer a sua validação. O módulo central responde com a informação relativa a autorização

da tag no quarto. Caso a tag seja a correta o módulo abre porta, caso contrario mantém a porta fechada.



**Figura 18 Arquitetura Software Módulo Central**

A Figura 18 descreve o algoritmo desenvolvido para o módulo central, este estabelece a comunicação com a Ethernet e controla os atuadores no interior do quarto de hotel. Seguindo esta lógica o módulo irá iniciar e realizaras suas configurações iniciais. De seguida valida se recebeu uma trama de tag NFC, caso tenha recebido vai validar a tag e se a tag estiver correta envia a trama para o módulo da porta com a informação para a porta abrir, caso a tag esteja incorreta envia a trama para a porta com a informação para manter a porta fechada. Após estas validações o sistema vai validar se recebeu algum comando Bluetooth caso tenha recebido faz o tratamento desse comando, por ultimo o sistema faz a atualização das variáveis no web server do hotel.

## 4. DESENVOLVIMENTO

Nesta secção será apresentado o protótipo funcional do sistema onde se evidenciará toda a informação relevante a nível de *hardware* e de *software* de modo a cumprir os objetivos inicialmente definidos, e o seu funcionamento. Tanto a nível de *hardware* como a nível de *software* será apresentada a sua construção e desenvolvimento, também estará apresentada a informação acerca dos módulos de comunicação presentes no trabalho, assim como, a explicação da implementação realizada, dos testes efetuados a cada aplicação e algumas informações que sejam necessárias para trabalhos futuros.

No seguimento do capítulo anterior, a descrição funcional do projeto vai ser dividida nos dois módulos constituintes do sistema, Fechadura e Central, em que para cada um será apresentado as características e particularidade de funcionamento de forma atingir os objetivos pretendidos para o projeto.

O detalhe dos componentes utilizados no trabalho vai de encontro com o nível de utilização dos mesmos, assim como, a sua complexidade dentro do projeto.

Será abordado também as diferentes comunicações que estão presentes no projeto entre cada componente, esquematizando-as de forma a ser compreendias, estas comunicação (*ZigBee*, *Bluetooth*) são essencialmente comunicações rádio frequência e comunicação série.

## 4.1. MÓDULO FECHADURA

O Módulo Fechadura é a placa elétrica da fechadura da porta do quarto de hotel, este módulo será alimentado por uma bateria de forma a garantir a sua autonomia, na placa do módulo estará os conectores da fechadura elétrica da bateria e também dos sinalizadores luminosos.

### 4.1.1. HARDWARE

Analisando os requisitos e objetivos pretendidos para o módulo da fechadura foi desenvolvido uma arquitetura para o módulo apresentado na Figura 19, com os componentes necessários interligados com o microcontrolador e com as ligações para os módulos de comunicação ZigBee e NFC.

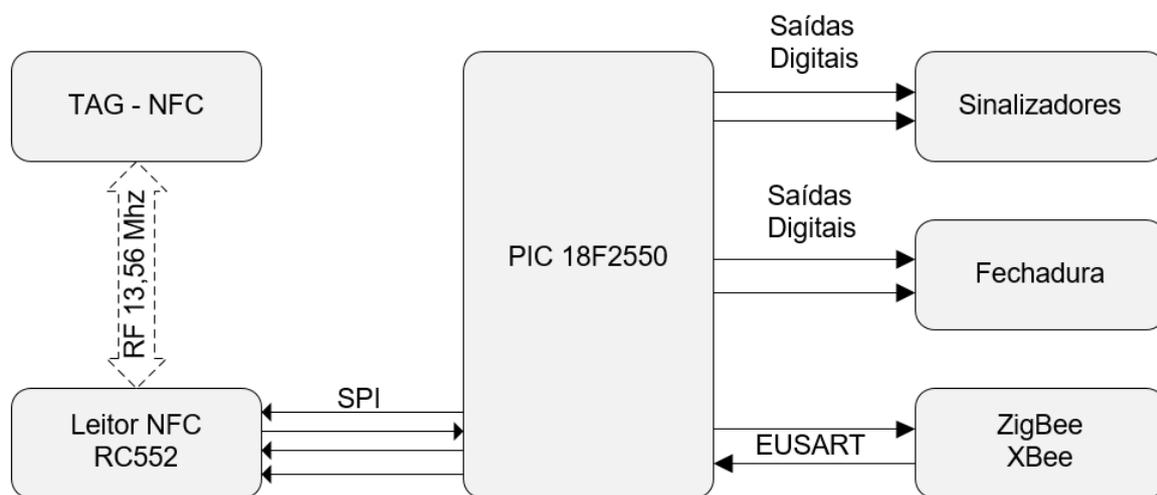


Figura 19 Arquitetura Módulo Fechadura

O microcontrolador escolhido para este módulo foi o PIC 18F2550, esta escolha foi baseada nos requisitos definidos para o módulo, tendo em consideração vários fatores, sendo eles, o intervalo de alimentação estar compreendido entre 2,0 V e 5,5 V, o que permite que seja alimentado a 3,3 V á imagem dos módulos de comunicação (NFC e ZigBee), a interfaces de comunicação necessárias para a interligação dos módulos de comunicação, ou seja, o módulo ZigBee comunica através da USART (*Universal Synchronous Asynchronous Receiver Transmitter*), enquanto que o módulo NFC comunica por SPI (*Serial Peripheral Interface*), o número de I/O e também tido em conta as dimensões físicas do componente, uma vez que a placa elétrica deverá ficar alojada na fechadura da porta.

As interfaces de comunicação, em seguida serão abordadas com mais detalhe devido á importância que representam neste módulo, sendo que a particularidade mais relevante é o fato do PIC 18F2550 ter o pino SDO (*Serial Data Output*) da interface SPI (pino 18) compartilhado com o pino RX (*Reception*) da interface USART.

O módulo USART do microcontrolador foi utilizado no modo assíncrono, com tramas de transmissão dados de 8 bits e com taxa de comunicação 9600 bps, utiliza os pinos RX e TX (*Transmission*) para estabelecer comunicação, o PIC 18F2550 possui o módulo EUSART (*Enhanced Universal Synchronous Asynchronous Receiver Transmitter*) que é uma USART com algumas funções adicionais (*Auto-wake-up* na recepção de dados, Calibração automática do *baud rate*, entre outras).

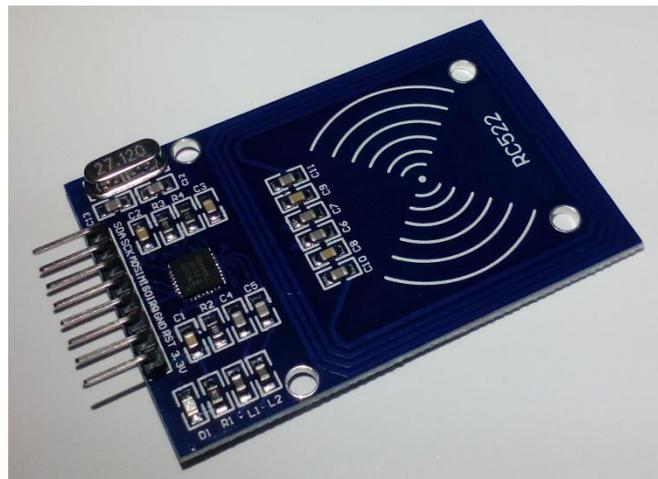
A interface SPI é uma comunicação síncrona que opera no modo *full-duplex*, está implementada no módulo MSSP (*Master Synchronous Serial Port*), este módulo pode operar no modo SPI ou no modo I<sup>2</sup>C (*Inter-Integrated Circuit*), uma vez que os dois modos compartilham o mesmo módulo, apenas uma delas pode ser ativa de cada vez. Os pinos da interface SPI são o SCK (pino de entrada ou saída de sinal *clock*), SDI (pino de entrada de dados), SDO (pino de saída de dados) e CS (pino de seleção).

Com já foi referido, o fato do microcontrolador partilhar um dos pinos nas duas interfaces de comunicação referidas anteriormente, foi necessário fazer a implementação da interface SPI por *software*, não sendo a única a solução possível para ultrapassar o problema, mas foi a solução que permitiu obter resultados mais rapidamente, facilitando a sua implementação. Através de um conjunto de funções do compilador C é possível implementar uma comunicação SPI em qualquer pino I/O do microcontrolador. Os pinos I/O usados para a implementação da comunicação SPI por *software* foram o RB2 para pino CS (*Chip Select*) do SPI, o RB3 para o pino SDI (*Serial Data Input*), o RB7 para o SDO e o RB6 para o pino SCK (*Serial Clock*).

Embora os problemas das interfaces de comunicação estejam ultrapassados, foi também necessário ter em atenção ao modo de programação utilizado, em todo o projeto foi utilizado o modo de programação ICSP (*In-Circuit Serial Programming*), como o nome indica programação do microcontrolador inserido no circuito da aplicação. Os pinos de programação do microcontrolador são o PGD (*Programming Data*) (RB7) e PGC (*Programming Clock*) (RB6), estes pinos são também os pinos utilizados para a comunicação

SPI, de forma a evitar que os sinais de programação não sejam afetados pelo circuito da aplicação, os dois pinos de programação precisam de ser isolados da restante aplicação, este isolamento pode ser obtido, usando uma resistência em série em cada pino, tipicamente o valor destas resistências é de 10 kohms. As resistências de isolamento não aparecem representadas na Figura 19 da arquitetura do módulo, contudo estão presentes no esquema elétrico do módulo, que será apresentado na Figura 23.

Os módulos de comunicação que já foram referidos anteriormente no capítulo 2, serão apresentados brevemente de seguida, onde se refere os aspetos importantes para o desenvolvimento do projeto. O módulo NFC Figura 20 é baseado no circuito MFRC522, da empresa NXP, bastante utilizado em comunicações de curta distância sem contato por rádio frequência, com uma frequência de 13,56 MHz, operam com taxas de transferência de dados de até 424 kbit/s, este circuito integrado suporta tags da série MIFARE.



**Figura 20 Módulo NFC – RC552**

O RC552 é módulo de baixo consumo e baixo custo, muito utilizado para a leitura e gravação de cartões, equipamentos inteligentes e dispositivos portáteis, entre outros. Este módulo funciona com tensão de 3,3 V e a comunicação é realizada por interface SPI com uma velocidade e comunicação de 10 Mbit/s, suporta cartões do tipo mifare1 S50/S70, mifare UltraLight, mifare Pro, mifare Desfire. Os pinos da placa são os pinos referentes á interface SPI (SCK, SDI, SDO e CS) um pino de *Reset* e os pinos de alimentação (VCC e GND (*Ground*)).

O módulo XBee, Figura 21 foi desenvolvido pela Digi, foi projetado para que possa funcionar de acordo com a norma IEEE 802.15.4 já apresentada anteriormente no capítulo

2. Os módulos XBee possuem comunicação sem fios com capacidade de ter consumos baixos relativamente às restantes comunicações sem fios, estes módulos implementam o protocolo ZigBee.

A comunicação realizada deste módulo é bastante fiável e estes operam dentro da banda de frequência ISM a 2.4GHz.



Figura 21 Módulo ZigBee – Xbee

De acordo com a Figura 22 é possível verificar que existem pinos de alimentação, pinos de comunicação, pinos de aquisição/atuação entre outros.

Pin #	Name	Direction	Description
1	VCC	-	Power supply
2	DOUT	Output	UART Data Out
3	DIN / <u>CONFIG</u>	Input	UART Data In
4	DO8*	Output	Digital Output 8
5	<u>RESET</u>	Input	Module Reset (reset pulse must be at least 200 ns)
6	PWM0 / RSSI	Output	PWM Output 0 / RX Signal Strength Indicator
7	PWM1	Output	PWM Output 1
8	[reserved]	-	Do not connect
9	<u>DTR</u> / SLEEP_RQ / DI8	Input	Pin Sleep Control Line or Digital Input 8
10	GND	-	Ground
11	AD4 / DIO4	Either	Analog Input 4 or Digital I/O 4
12	<u>CTS</u> / DIO7	Either	Clear-to-Send Flow Control or Digital I/O 7
13	ON / <u>SLEEP</u>	Output	Module Status Indicator
14	VREF	Input	Voltage Reference for A/D Inputs
15	Associate / AD5 / DIO5	Either	Associated Indicator, Analog Input 5 or Digital I/O 5
16	<u>RTS</u> / DIO6	Either	Request-to-Send Flow Control, or Digital I/O 6
17	AD3 / DIO3	Either	Analog Input 3 or Digital I/O 3
18	AD2 / DIO2	Either	Analog Input 2 or Digital I/O 2
19	AD1 / DIO1	Either	Analog Input 1 or Digital I/O 1
20	AD0 / DIO0	Either	Analog Input 0 or Digital I/O 0

Figura 22 Descrição dos Pinos do Módulo XBee

Para transmitir informação entre módulos XBee utiliza-se os pinos de UART (*Universal Asynchronous Receiver Transmitter*) de cada um dos módulos. Para enviar informação para o módulo é necessário ter algum dispositivo com interface UART para realizar essa comunicação com o módulo. Esse dispositivo poderá ser um microcontrolador ou um computador, é necessário ter atenção que a interface UART existente utiliza a logica CMOS (*Complementary Metal-Oxide-Semiconductor*) (tensões entre 2,8 e 3,4V). Após esta interface ser garantida o microcontrolador poderá trocar informações com o módulo XBee.

Contudo, de acordo com arquitetura do módulo, existe também saídas digitais para a atuação sobre a fechadura da porta para a abertura e atuação sobre sinalizadores luminosos, estes sinalizadores assumem dois estados, verde quando a abertura da fechadura é realizada ou vermelho que é o estado sempre que a fechadura elétrica da porta não é ativa pelo sistema. As saídas digitais são os portos I/O do microcontrolador utilizado.

Concluída toda a explicação sobre a arquitetura de hardware desenvolvida para o módulo, assim como, explicação de alguns componentes principais, será também apresentado e explicado o esquema elétrico do módulo da fechadura. Na Figura 23, encontra-se ilustrado o circuito elétrico realizado.

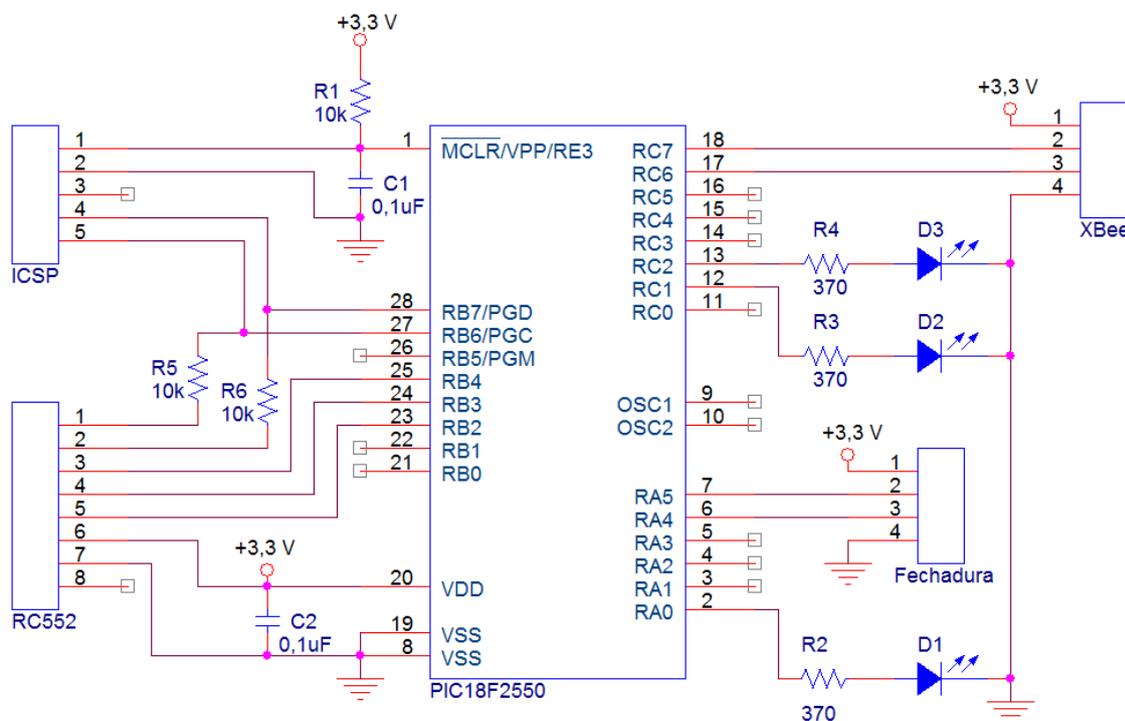


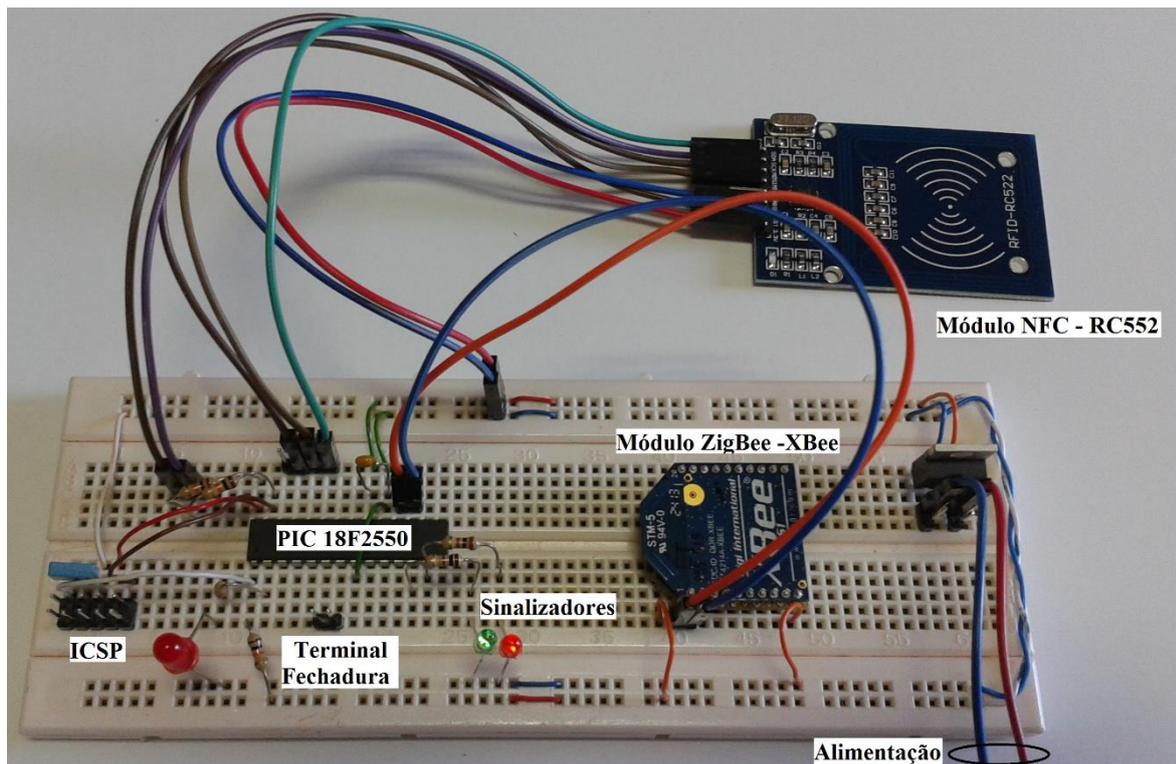
Figura 23 Circuito Elétrico Módulo Fechadura

No circuito elétrico apresentado está representado todas as ligações entre o microcontrolador e os diversos componentes do circuito. Os módulos de comunicação estão representados por conectores NFC (RC552) e XBee respetivamente, de forma a tornar o circuito mais simples para melhor interpretação, pois o esquema elétrico de cada módulo não alvo de desenvolvimento do projeto.

Como referido anteriormente, o modo de programação utilizado foi o ICSP, no seguimento deste modo de programação foi criado o conector de programação que aparece representado no circuito com a mesma descrição (ICSP), através deste conector é possível programar facilmente o microcontrolador sem o retirar do circuito em que está inserido. Para isso, foi necessário inserir no circuito resistências de isolamento representados por R5, nas linhas de programação de forma a isolar o circuito de programação da restante aplicação, isto deve-se, como já mencionado, a partilha dos pinos de programação. Note-se que os pinos RB7 e RB6 do microcontrolador são utilizados para o leitor NFC e pelo circuito de programação. Esta otimização de pinos permite deixar mais pinos livres para desenvolvimentos futuros.

Por ultimo, os sinalizadores luminoso que são referidos na arquitetura do módulo da fechadura, estão representados no circuito pelas resistências R2, R3, R4 e os díodos emissores de luz D1, D2, D3. No caso da fechadura, está representado por um conector que disponibiliza duas saídas digitais e alimentação, permitindo assim adaptar a qualquer fechadura elétrica.

De forma a comprovar todo o funcionamento do módulo desenvolvido, o circuito elétrico foi montado e testado numa placa de testes, como está representado na Figura 24.



**Figura 24 Montagem do circuito elétrico do módulo Fechadura**

Na montagem apresentada, é possível identificar todos os componentes referidos anteriormente através dos identificadores, nos barramentos de alimentação da placa a tensão é de 3,3 V. O fato de todo o circuito ser alimentado a 3,3 V, torna o módulo mais interessante, pois sendo um baixo nível de tensão facilita escolha da bateria e a sua manutenção para o funcionamento autónomo na porta.

Na montagem foram realizados diversos testes ao módulo, testes gerais ao módulo e testes individuais aos componentes utilizados, assim sendo, a descrição dos testes realizados vai ser dividida em duas grupos, sendo eles:

- Teste Individuais de Componentes:
  - Programação do microcontrolador inserido no circuito;
  - Leitura de tags NFC através do respetivo módulo;
  - Comunicação do XBee entre o módulo da Fechadura e módulo Central;

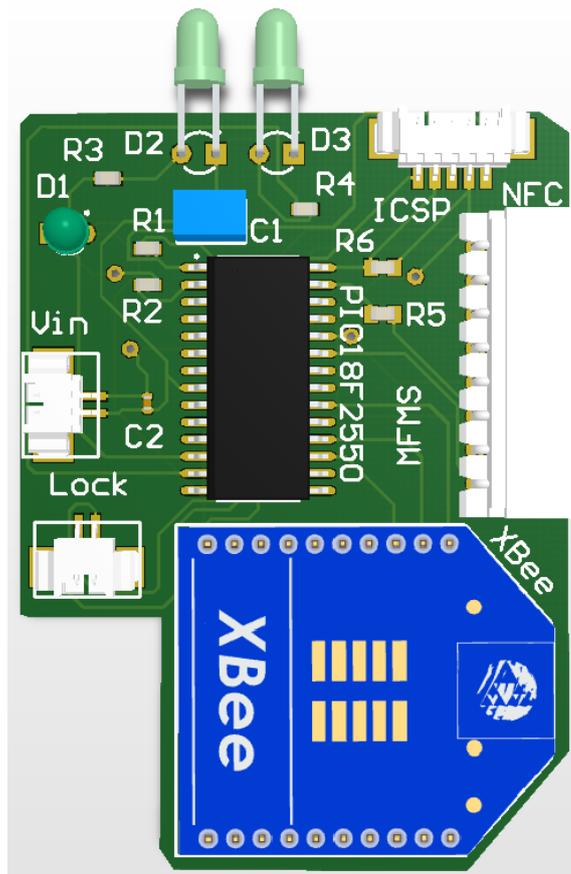
- Testes Gerais do Módulo Fechadura:
  - Leitura da tag NFC, construção da trama de dados XBee e envio da trama para o módulo central;
  - Receção da resposta do módulo central e seu processamento, abertura da porta e a sua sinalização;

Os testes realizados ao módulo provam o funcionamento pretendido, no qual responde ao objetivos definidos para o mesmo. Desta forma, foi validado todas as opções tomadas no desenvolvimento do *hardware* do módulo.

Ao longo deste subcapítulo foram apresentadas e explicadas as diferentes fases de desenvolvimento do módulo da fechadura, inicialmente foi feita uma abordagem geral do módulo, explicação dos diferentes componentes, e interligações entre eles, onde foi sempre dando ênfase às opções de desenvolvimento tomadas para cumprir os objetivos. De seguida foi documentada a implementação desenvolvida para este módulo, desde da apresentação do circuito elétrico passando pela montagem de todo o circuito e em placa de testes, terminando nos testes reais da solução desenvolvida.

Após terem sido apresentados os testes realizados de forma a garantir o funcionamento correto do módulo, será apresentada de seguida a prototipagem do módulo da fechadura. A placa desenvolvida trata-se da placa de controlo da fechadura da porta do quarto de hotel. A placa de circuito impresso desenvolvido está ilustrada na Figura 25, pela análise da figura é possível identificar todos os componentes do módulo, no caso do leitor NFC apenas esta o conector de ligação (NFC), pois este deve estar alojado junto a face exterior da fechadura para ser possível a leitura no exterior do quarto.

As fechaduras serão totalmente controladas pela placa desenvolvida, no protótipo desenvolvido possui conector de alimentação (*Vin – Voltage Input*), que deve ser ligado diretamente às baterias comuns das fechaduras elétricas dos quartos de hotéis. O conector da fechadura elétrica também está visível na placa (*Lock*), por último o conector (ICSP) trata-se do conector de programação do microcontrolador. Para além destes conectores existentes, também é possível facilmente identificar alguns componentes eletrónicos na Figura 25, salientar que o módulo XBee ficara soldado diretamente na PCB (*Printed Circuit Board*).



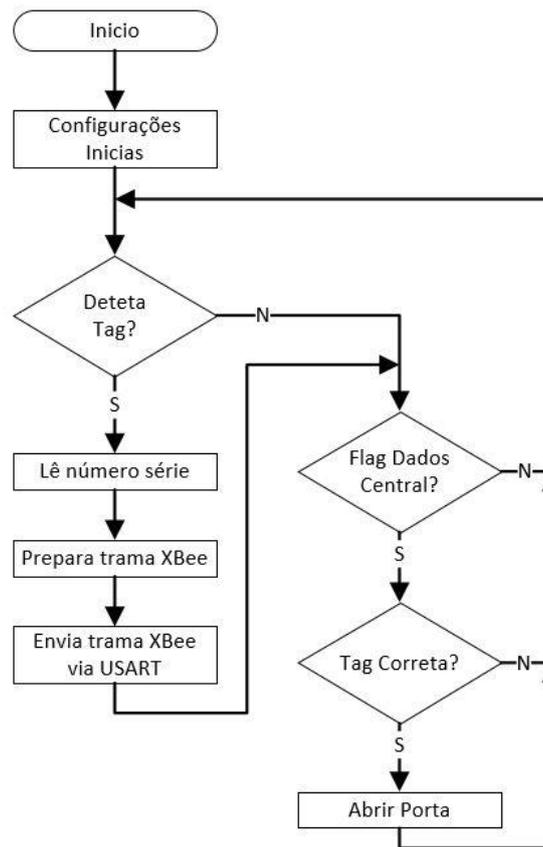
**Figura 25** Montagem do módulo Fechadura em PCB

A placa foi desenhada com recurso ao *software* CircuitMaker, onde foi contruído o esquema elétrico da placa e de seguida o desenho da placa de circuito impresso, do qual foi retirada a visualização 3D, o Anexo A disponibiliza diferentes perspetivas de visualização da placa.

#### **4.1.2. SOFTWARE**

No seguimento da apresentação *hardware* desenvolvido, o *software* está perfeitamente alinhado com todo esse desenvolvimento, complementando as decisões tomadas para o *hardware*. De forma a demonstrar o funcionamento do *software*, a explicação vai ser dividida no fluxograma do programa principal e fluxograma do serviço de interrupções do microcontrolador.

O fluxograma ilustrado na Figura 26 representa o funcionamento do programa principal deste módulo. O *software* desenvolvido permite que o microcontrolador funcione de forma autónoma e com interação com o módulo central, de forma a permitir a abertura da porta do quarto de hotel.



**Figura 26 Fluxograma do programa principal do módulo Fechadura**

O programa desenvolvido começa pela definição de variáveis necessárias para a construção do código e com as respetivas configurações de registos dos periféricos utilizados do microcontrolador (Oscilador, Portos I/O, USART, SPI, Interrupções). As configurações dos registos são a base para o correto funcionamento do *software* elaborado.

Após esta configuração, são executadas funções necessárias para a configuração e parametrização do leitor NFC (MFRC522), de salientar que as funções utilizadas para a configuração e comunicação com o leitor utilizado foram adaptadas da referência documental [29], durante as pesquisas realizadas para o desenvolvido do projeto foi encontrado este documento, no qual o autor disponibiliza um programa exemplo com funções já validadas para a comunicação com o leitor. Estas funções foram adaptadas á necessidade do módulo da fechadura, ou seja, a leitura da tag NFC foi ajustada á informação pretendida do resultado dessa leitura (formato e composição da trama de dados), nessa função de leitura da tag NFC foi também acrescentado código para a geração e envio das tramas de dados do XBee, contudo para além das funções adaptadas foram utilizadas funções de controlo de comunicação e deteção de erros da comunicação disponibilizadas pelo autor.

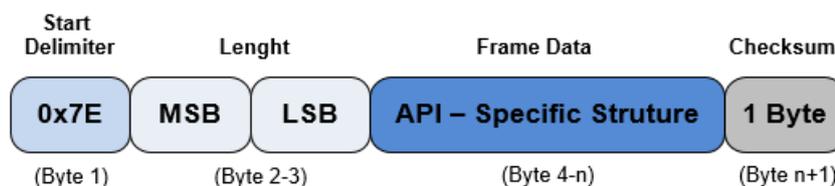
Desta forma foi possível obtenção de resultados da comunicação com o módulo RC522 mais rapidamente.

Assim o *software* desenvolvido esta preparado para sempre que deteta uma tag, faz a sua leitura da tag NFC e com o resultado desta leitura é feita a construção da trama de dados e enviada para o XBee pelo periférico USART. Depois do envio dos dados referentes a leitura da tag o módulo da fechadura aguarda por uma resposta do módulo central, quando a resposta e detetada é analisada e caso seja indicado a abertura da porta são atuadas as saídas digitais necessárias para esse efeito, caso contrario a porta mantém-se fechada.

Seguidamente será feita uma abordagem sobre as tramas de comunicação utilizadas para a comunicação entre os módulos XBee, estas tramas de dados utilizadas estão diretamente relacionadas com o modo de operação escolhido para o módulo XBee. Por defeito o XBee opera no modo transparente, quando funcionam neste modo todos os dados recebidos na UART do XBee através dos pinos de comunicação, ficam em fila de mensagens para serem transmitidos por rádio frequência, quando são recebidos dados via rádio frequência os dados são enviados para esses pinos.

A operação API (*Application Programming Interface*) é uma alternativa á operação transparente, quando o módulo opera no modo API todos os dados que entram e saem do módulo estão contidos em tramas que definem operações ou eventos dentro do módulo. Esta operação permite transmitir dados para vários destinos, receber o estado de sucesso ou de falha de transmissão de cada pacote de dados e ainda identificar o endereço de origem de cada pacote recebido. Este foi o modo de operação utilizado para a comunicação entre os módulos fechadura e central.

A Figura 27 mostra a estrutura geral das tramas de dados API.



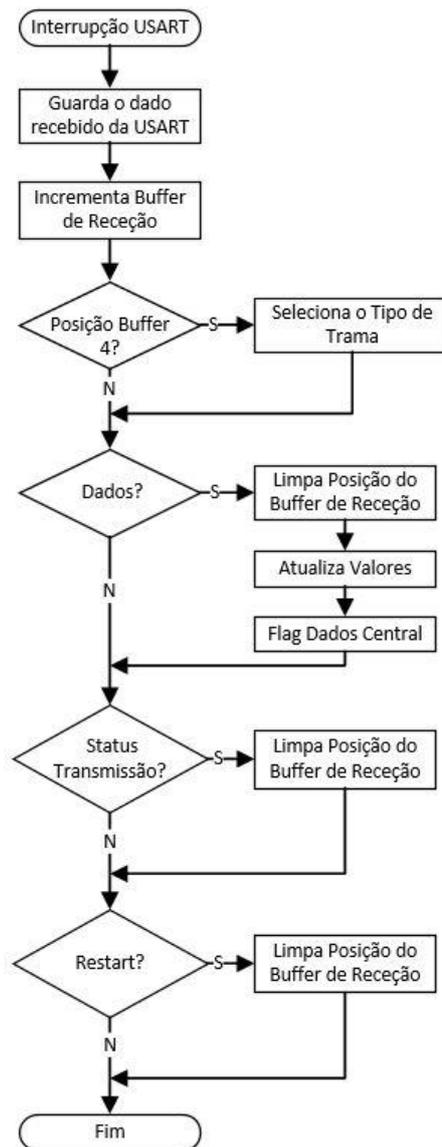
**Figura 27 Trama de dados no modo API**

A trama inicia com um *byte* delimitador de início de trama (0x7E), de seguida são introduzidos dois *bytes* MSB (*Most Significant Byte*) e LSB (*Least Significant Byte*), onde especifica o tamanho da trama de dados (*Lenght*), de seguida vem a trama de dados (*Frame Data*) que depende do tipo de trama que se pretende enviar, a trama de dados possui uma estrutura específica dependendo do tipo de ação/informação transmitida, no final da trama de dados é enviado um *byte* como o campo de *checksum* para teste de integridade dos dados.

A trama apresentada é gerada após cada leitura, assim sendo, a criação deve ser dinâmica de forma a conseguir enviar todas as tags lidas, para isso foi desenvolvida uma função que gera a trama, de acordo com a estrutura descrita e faz o cálculo dinâmico do comprimento da trama de dados e o cálculo do *checksum*.

No seguimento do modo de operação utilizado, o módulo XBee envia para o microcontrolador mais tramas para além das que recebe do módulo central, ou seja, envia tramas de *restart* quando o módulo liga ou é reiniciado e também recebe tramas de *status* da transmissão de dados, estas tramas de dados são lidas e processadas pelo microcontrolador. Para otimizar este processo foi configurado a receção de dados da USART por interrupção, assim o serviço de interrupção faz o tratamento de todas as tramas recebidas.

O fluxograma ilustrado na Figura 28, representa o funcionamento do serviço de interrupção para a receção de dados pela USART.



**Figura 28 Fluxograma do serviço de interrupções do módulo da fechadura**

Sempre que a *flag* de recepção de dados por interrupção é ativa o programa entra na interrupção e faz a leitura do *byte* recebido, mediante o número do *byte* recebido é feita a validação do tipo de trama que esta que o microcontrolador está a receber. Os vários tipos de tramas referidos anteriormente, assumem tamanhos diferentes, contudo o tipo de trama é definido pelo *byte* número 4 da trama de dados API apresentada (*Frame Data*). Todos os dados recebidos são validados, ou seja, quando é recebida a trama de dados API, os valores são guardados e é feito um controlo dos *bytes* recebidos de forma a validar a integridade dos dados, após esta validação é ativa um *flag* de “dados corretos”, através desta *flag*, o programa principal do microcontrolador processa a informação recebida. No fim de cada serviço de interrupção a *flag* de recepção de dados da USART é limpa.

## 4.2. MÓDULO CENTRAL

O módulo central desenvolvido foi pensado para ser um módulo pertencente ao quadro elétrico de cada quarto do hotel, desta forma será fácil a alimentação deste módulo assim como torna mais simples a ligação aos atuadores elétricos dos periféricos controlados pelo módulo. O módulo tem como objetivo ser de fácil manutenção para garantir o funcionamento pleno.

### 4.2.1. HARDWARE

Analisando os requisitos e objetivos definidos para o módulo central foi desenvolvido uma arquitetura para o módulo apresentado na Figura 29, que em conjunto com o módulo da fechadura formam um sistema de controle para o quarto de hotel. No diagrama apresentado estão representados todos os componentes necessários para o desenvolvimento do módulo, salientar que foram necessários dois microcontroladores de forma a gerir todas as comunicações envolvidas no módulo em conjunto com o multiplexer. Nesse sentido os circuitos de cada microcontrolador foram legendados de circuito Ethernet e circuito central.

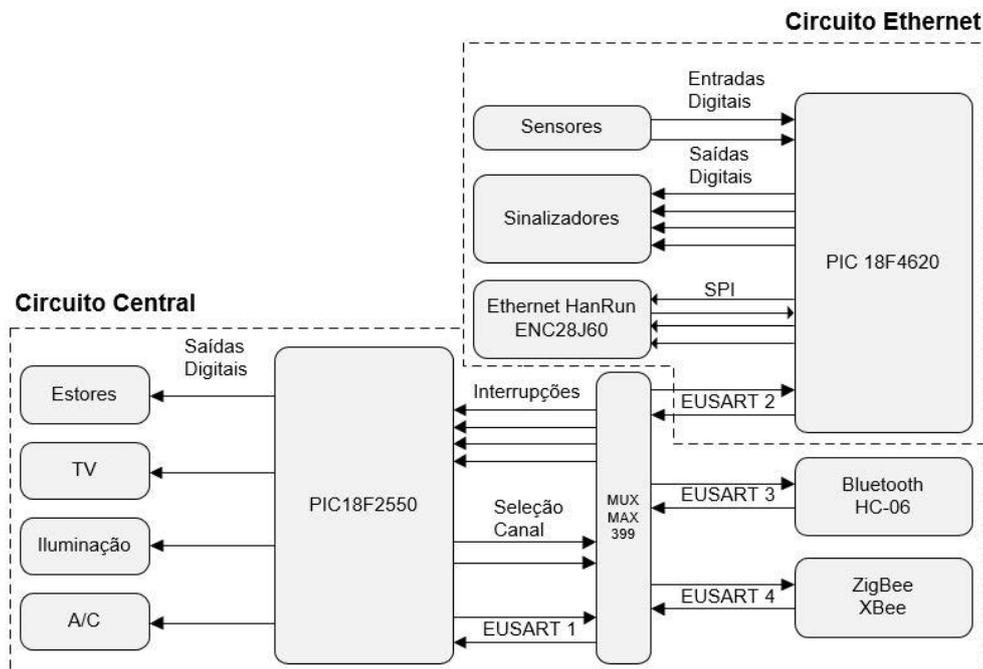


Figura 29 Arquitetura do Módulo Central

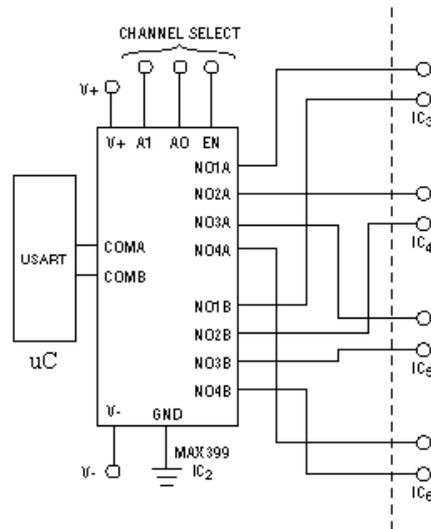
Neste módulo existem três meios de comunicação distintas, este fator influenciou algumas das opções tomadas para o desenvolvimento deste módulo, principalmente pelas interfaces de comunicação que cada módulo dispõe para a comunicação com o microcontrolador. Os

módulos Bluetooth e XBee comunicam através da USART, enquanto que o módulo Ethernet comunica através de SPI.

Assim sendo, foi utilizado o PIC 18F2550 à imagem do módulo da fechadura, este microcontrolador faz o controlo de todas as interfaces de comunicação, contudo possui apenas uma porta USART. Desta forma, o controlo das comunicações é feito através de um circuito multiplexer, Figura 30. Este microcontrolador faz também o controlo dos periféricos do quarto (A/C, Iluminação, TV e Estores), este controlo é representado e demonstrado por saídas digitais.

O segundo microcontrolador utilizado neste módulo foi o PIC 18F4620, este microcontrolador foi escolhido principalmente pela sua memória de programa de 64 kbs, esta necessidade deve-se ao fato da compilação da *stack* TCP/IP (*Transmission Control Protocol/Internet Protocol*) da microchip ocupar bastante espaço de memória. Este microcontrolador é responsável pela comunicação Ethernet através do respetivo módulo. Neste microcontrolador existem também ligados alguns sinalizadores luminosos que funcionam como *status* de funcionamento da comunicação Ethernet, contudo o microcontrolador faz a leitura de dois sensores, sendo eles *switches* simples para o sistema saber o estado da porta e da janela (aberto/fechado). A utilização deste microcontrolador foi para uso exclusivo da comunicação Ethernet de forma a isolar das restantes comunicações devido a sua complexidade, desta forma foi possível obter resultados positivos e eficazes mais rapidamente. A comunicação entre as duas PIC é pela USART através do circuito multiplexer.

Os microcontroladores utilizados neste trabalho, possuem apenas uma USART, contudo existe necessidade de vários módulos comuniquem com o mesmo microcontrolador através da mesma USART. Através do circuito multiplexer, torna-se possível que o módulo Bluetooth e o módulo XBee comuniquem com o mesmo microcontrolador através do mesmo periférico de comunicação, o módulo da Ethernet comunica por SPI e está isolado no PIC 18F4620, por sua vez, os dois microcontroladores comunicam entre si pela USART. O circuito multiplexer implementado aparece ilustrado na Figura 30, note-se que o exemplo apresentado permite partilhar a USART com quatro circuitos (IC<sub>3</sub>, IC<sub>4</sub>, IC<sub>5</sub>, IC<sub>6</sub>), contudo apenas foram utilizados três circuitos para este projeto.



**Figura 30** Circuito multiplexer da USART, adaptado de [30]

O circuito integrado MAX 399 utilizado neste projeto é um multiplexer de precisão, com uma rápida velocidade de comutação entre os canais (tempo de transição menos de 250 ns) permite obter bons resultados na comunicação, a tensão alimentação do integrado pode ser entre +3 V até +15 V, este intervalo permite que seja alimentado a +3,3 V, á imagem da maioria dos restantes componentes deste módulo.

O circuito apresentado na Figura 30 funciona como multiplexer e também como demultiplexer, isto deve-se ao fluxo de comunicação, o multiplexe é o envio de vários sinais de diferentes circuitos para um único circuito, enquanto que o demultiplexer é o oposto envio de sinais de um único circuito para vários circuitos diferentes. No projeto desenvolvido, estes processos estão presentes, ou seja, a comunicação presente neste módulo é bidirecional, ocorre módulo da fechadura para módulo central e vice-versa, assim como também as comunicações Bluetooth e Ethernet.

Para que todos os fluxos de comunicação sejam possíveis o PIC 18F2550 faz a seleção do canal pretendido através de saídas digitais do microcontrolador de acordo com algoritmo implementado, de forma a enviar ou receber a informação de qualquer circuito ligado ao MAX 399. Na Tabela 4 está representado a combinação de sinais para a seleção de cada canal do multiplexer, a seleção é feita pelos sinais de A0 e A1, dependendo do sinal EN (*Enable*) que permite que a seleção seja válida sempre que esteja ativo.

**Tabela 4 Seleção de Canal MAX 399**

EN	A1	A0	Canal
0	X	X	-
1	0	0	Canal 1 (IC3) – n/c
1	0	1	Canal 2 (IC4) – Bluetooth
1	1	0	Canal 3 (IC5) – XBee
1	1	1	Canal 4 (IC6) – Ethernet

A seleção de canal é feita antes de iniciar qualquer comunicação, independentemente do sentido que ocorre. Quando a comunicação é do microcontrolador para qualquer módulo de comunicação, a seleção do canal é feita assim que seja necessário iniciar a comunicação, quando a comunicação é dos módulos de comunicação para o microcontrolador, antes deste iniciar a recepção de dados a seleção do respectivo canal deve ocorrer, para isso foi utilizado as interrupções externas do microcontrolador, que são ativas assim que os módulos de comunicação iniciam a comunicação com o microcontrolador através do MAX 399, estas linhas de interrupções externas aparecem representadas na Figura 29.

Os módulos de comunicação que tem vindo a ser referidos neste módulo, serão de seguida apresentados brevemente, onde se refere os aspetos importantes para o desenvolvimento deste projeto. O módulo XBee utilizado no módulo central é igual ao XBee do módulo da fechadura, como já foi apresentado anteriormente não será feita nenhuma explicação do mesmo.

O módulo *Bluetooth* HC-06, apresentado na Figura 31, é um módulo de classe 2 de baixo custo e baixo consumo. Funciona apenas em modo *slave* (escravo), ou seja, permite que outros dispositivos se conectem a ele, mas não permite que ele próprio se conecte a outros dispositivos *Bluetooth*. A comunicação deste módulo está dentro da banda de frequência ISM a 2.4GHz.



**Figura 31 Módulo Bluetooth HC-06**

As configurações de fábrica do módulo HC-06 são as seguintes:

- *Baud rate*: 9600 bps
- *Data bits*: 8
- *Parity*: N
- *Stop bit*: 1
- *ID*: Linvor
- *Password*: 1234

Os parâmetros de fábrica podem ser alterados, esta alteração é realizada através de comandos AT e antes de o módulo ficar emparelhado com outro dispositivo, ou seja, enquanto o led de *status* esta intermitente (o led a piscar significa que não esta emparelhado com dispositivo). Depois de emparelhado a outro dispositivo *Bluetooth*, o HC-06 funciona de forma transparente e não aceita comandos AT.

O módulo HC-06 possui quatro pinos de ligação física, a descrição dos pinos esta descrito na Tabela 5.

**Tabela 5 Pinos de ligação do módulo HC-06**

<b>Pino</b>	<b>Descrição</b>
VCC	Alimentação (3,6 V a 6V)
GND	Ground
TX	Saída de dados (nível de tensão 3,3 V)
RX	Entrada de dados (nível de tensão 3,3 V)

O módulo Ethernet utilizado neste desenvolvimento e que tem vindo a ser referido ao longo do relatório foi o ENC28J60, trata-se de um controlador Ethernet autónomo com interface SPI.

O ENC28J60 é compatível com a especificação IEEE 802.3, possui MAC integrado e camada física 10BASE-T, incorpora uma série de filtros para limitar os pacotes de dados que necessitam de ser processados. Possui também um módulo interno DMA (*Direct Memory Access*) de transferência rápida de dados e assistente de *hardware* para o cálculo de *checksum*, que é usado em vários protocolos de rede. A comunicação com o microcontrolador é feita através de um pino de interrupção externa e a interface SPI, com taxas de dados de 10 Mbps e uma taxa de *clock* de 20 MHz.

Uma das montagens mais comuns com este módulo Ethernet está apresentado na Figura 32

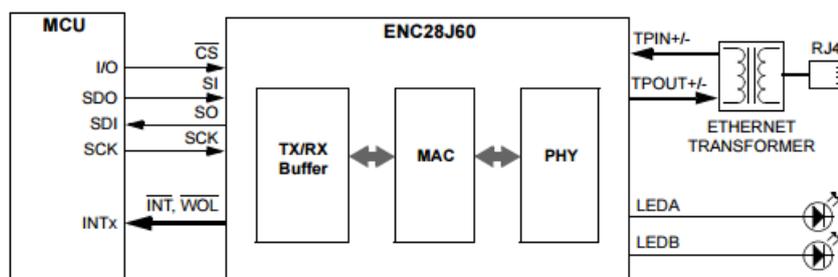


Figura 32 Montagem do ENC28J60 [33]

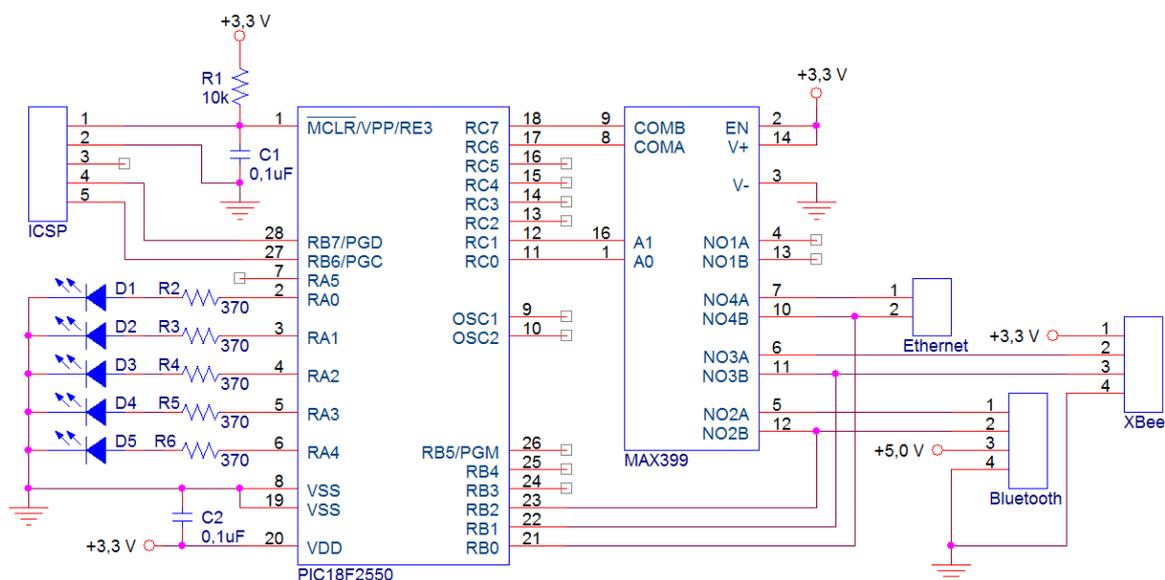
O módulo Ethernet utilizado está apresentado na Figura 33, trata-se de uma placa com a montagem do circuito apresentado anteriormente, esta placa é composta pelo ENC28J60, um cristal, um conector de 10 pinos, ainda o conector Ethernet RJ45 que possui dois leds que indicam a atividade da rede, assim como estão também presentes outros componente passivos necessários para interligar o controlador a rede Ethernet.

O conector de 10 pinos que a placa dispõe possui as linhas VCC e GND para alimentação do circuito de 3,3 V e os pinos do barramento SPI (CS, INT (*Interruption*), SDI, SDO, SCK), que permitem a interligação desta placa com o microcontrolador responsável pela comunicação do módulo central com a Ethernet.



**Figura 33 Módulo Ethernet – ENC28J60**

Concluída toda a explicação sobre a arquitetura de hardware desenvolvida para o módulo, assim como, explicação de alguns componentes principais, será também apresentado e explicado o esquema elétrico do módulo central que complementa a arquitetura de hardware. Devido a dimensão do circuito, este foi dividido em dois circuitos de forma a tornar mais fácil a sua apresentação no relatório e por sua vez facilitando a interpretação e explicação, como já referido anteriormente os circuitos foram divididos em circuito central e *Ethernet*. Na Figura 34 encontra-se ilustrado o esquema elétrico central do módulo central.



**Figura 34 Circuito Elétrico Módulo Central – Circuito Central**

O circuito elétrico apresentado traduz e complementa parte dos objetivos definidos para este módulo, este circuito desempenha duas funções principais no módulo central, a ligação

elétrica de todos os módulos de comunicação com o microcontrolador e também a representação das ligações para atuação dos periféricos do quarto.

O microcontrolador e os módulos de comunicação estão interligados pela USART, através do multiplexer (MAX399), permitindo a comunicação possível com qualquer dos módulos desde que feita a seleção correta do respetivo canal, a seleção de canal é feita pelo microcontrolador com duas saídas digitais. Os três módulos de comunicação (Ethernet, XBee, Bluetooth), estão representados no circuito elétrico por conetores. O módulo Ethernet é a segunda parte do circuito elétrico do módulo central, que será explicada em seguida, este possui um microcontrolador dedicado para comunicação a Ethernet, por essa razão a ligação é semidirecta entre as duas USART dos dois microcontroladores (PIC18F2550 e PIC18F4620).

O módulo XBee está representado por um conector de quatro terminais, á imagem do circuito elétrico do módulo Fechadura, este conector dispõe de duas linhas de alimentação (3,3 V) e duas linhas de comunicação. O módulo Bluetooth também esta representado por um conector de quatro terminais, duas de alimentação e duas de comunicação. Salientar que este módulo é alimentado a uma tensão de 5 V e a comunicação assume níveis de tensão de 3,3 V.

O microcontrolador quando recebe dados pela USART deve previamente saber a sua origem, para isso as linhas de receção de dados de cada módulo de comunicação foram ligadas aos pinos de interrupções externas do microcontrolador (RB0, RB1, RB2), no circuito elétrico estão representadas essas ligações.

No circuito elétrico apresentado as ligações do microcontrolador com os atuadores elétricos dos periféricos do quarto (Iluminação, Estores, TV e A/C) aparecem representados por circuitos Led ligados a saídas digitais do microcontrolador. Estes circuitos simples permitiram testar e comprovar o funcionamento do sistema, contudo, as saídas digitais podem ser ligadas a circuitos de potência que controlem sistemas reais existentes no quarto.

No seguimento da abordagem dos circuitos de potência, serão referidos dois circuitos que permitem que o microcontrolador faça o controlo dos periféricos apresentados por meio de saídas digitais. Os circuitos referidos são o controlo de cargas por Relé e o controlo por TRIAC (*Triode for Alternating Current*), o circuito elétrico de cada um aparece ilustrado na Figura 35. Os dois circuitos estão na mesma figura, contudo estão devidamente legendados que facilmente permitem a sua identificação.

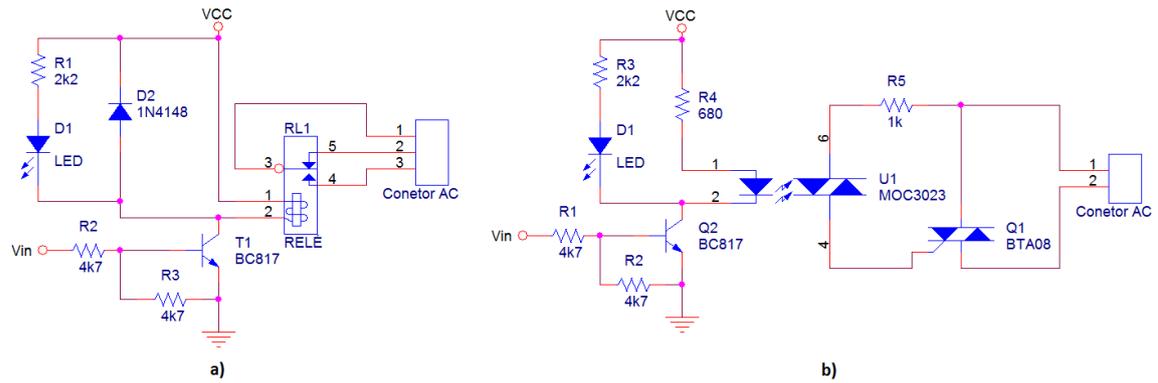


Figura 35 Circuitos de Potência - a) Circuito Relé b) Circuito TRIAC

Os dois circuitos permitem atuar sobre um circuito de corrente alternada, apenas com uma saída digital do microcontrolador, estes circuitos são facilmente atuados com impulsos digitais com tensão de 3,3 V. Por último, no circuito elétrico principal aparece também representado o conector ICSP, referente a programação do microcontrolador, explicado anteriormente no módulo da fechadura.

O circuito elétrico *Ethernet* aparece ilustrado na Figura 36.

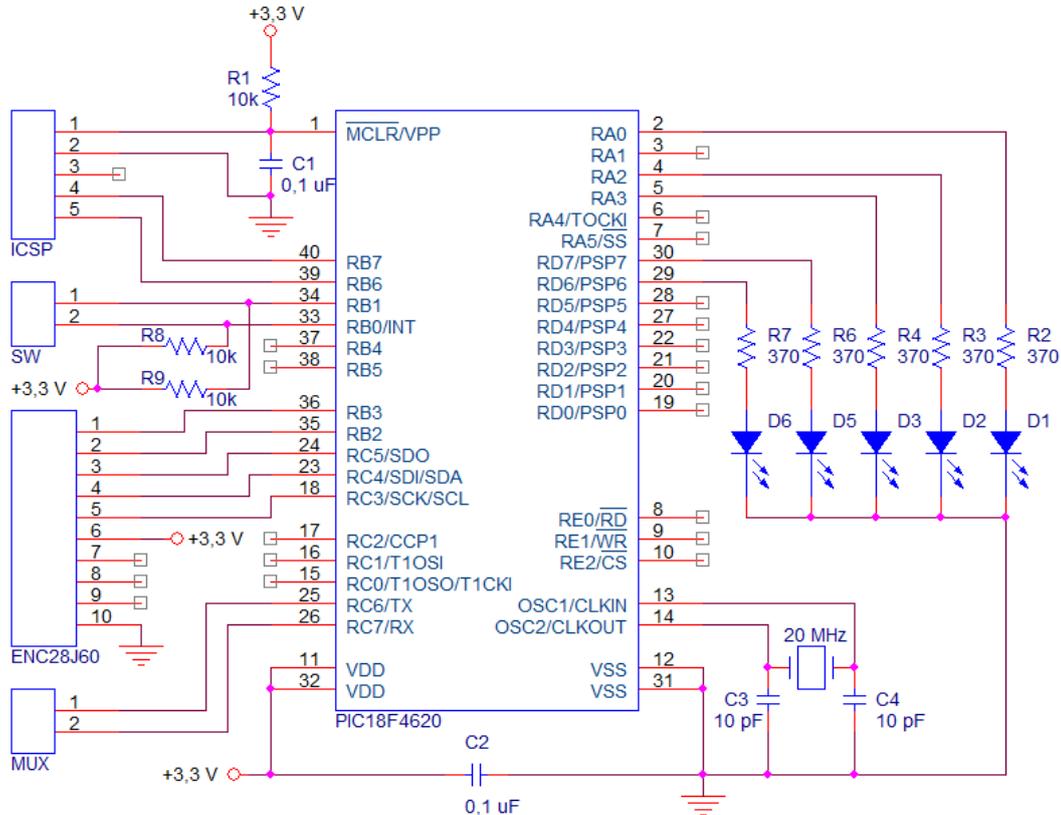


Figura 36 Circuito Elétrico Módulo Central – Circuito Ethernet

Este circuito é o esquema elétrico do microcontrolador PIC 18F4620 e do módulo Ethernet. O módulo de comunicação Ethernet está representado no esquema por um conector com a designação ENC28J60, neste conector estão disponíveis as linhas de comunicação do barramento SPI, que é a interface de comunicação entre o microcontrolador e a placa Ethernet, assim como, também estão disponíveis as linhas de alimentação do módulo (3,3 V)

Neste circuito estão também representados os sinalizadores luminosos para demonstração de status da comunicação e funcionamento do módulo Ethernet. Este módulo disponibiliza também de duas entradas digitais com o objetivo de fazer leitura do estado da janela e da porta (Aberto ou Fechado). Este microcontrolador à imagem de todos os outros, é programado através do conector ICSP.

O fato de o algoritmo implementado neste microcontrolador ser exigente a nível de processamento, foi necessário definir o sinal de relógio externo através de um cristal de quartzo, de forma a responder ao servidor implementado no microcontrolador.

Os microcontroladores deste módulo estão interligados entre si pela USART, que está disponível no conector Ethernet apresentado no circuito.

De forma a comprovar todo o funcionamento do módulo desenvolvido, os circuitos elétricos foram montados e testados em placas de testes, na Figura 37 está ilustrado a montagem da primeira parte do circuito elétrico, a imagem está legendada de forma a identificar todos os componentes relevantes do circuito. Salientar a identificação dos cabos elétricos RX/TX referente a comunicação USART entre as duas partes do circuito e os cabos elétricos das linhas das interrupções externas. Nesta parte do circuito apenas o módulo Bluetooth é alimentado a 5 V, todo o restante circuito funciona com tensão de alimentação de 3,3 V.

A montagem da segunda parte do circuito aparece ilustrado na Figura 38, esta imagem também possui legendas para a identificação de todos os componentes relevantes do circuito elétrico, sendo também facilmente identificado os cabos elétricos RX/TX da comunicação entre os dois microcontroladores deste módulo. Esta montagem funciona com alimentação de 3,3 V.

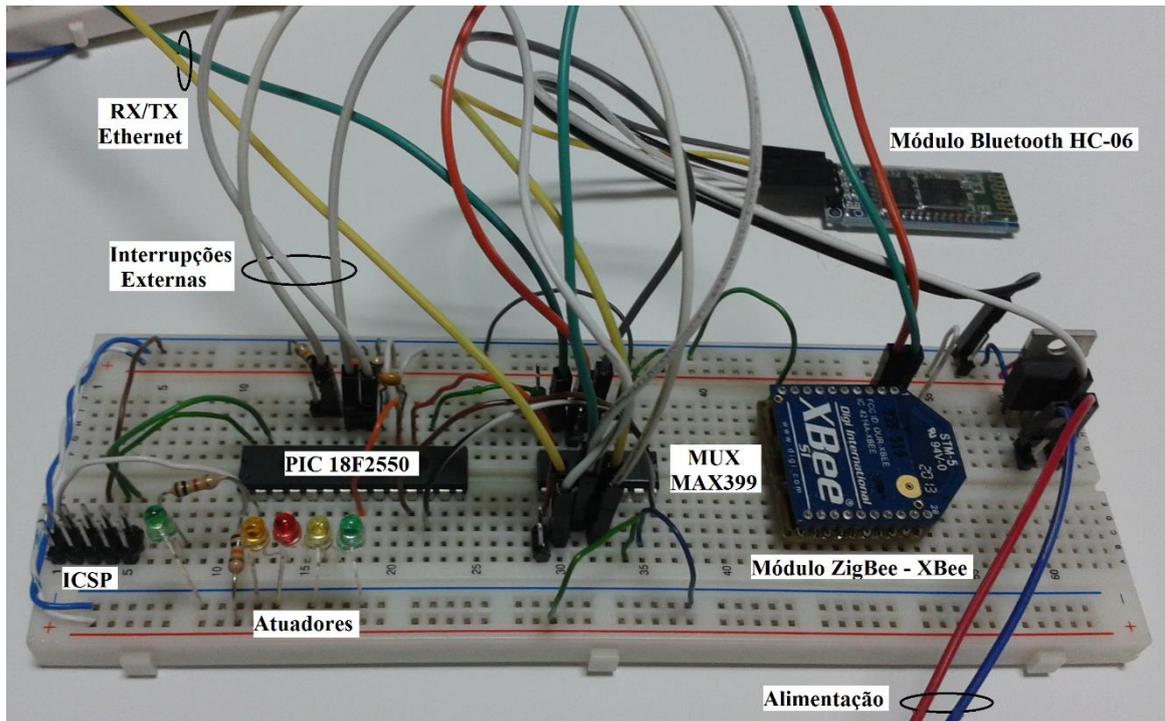


Figura 37 Montagem do Circuito Elétrico do Módulo Central – Circuito Central

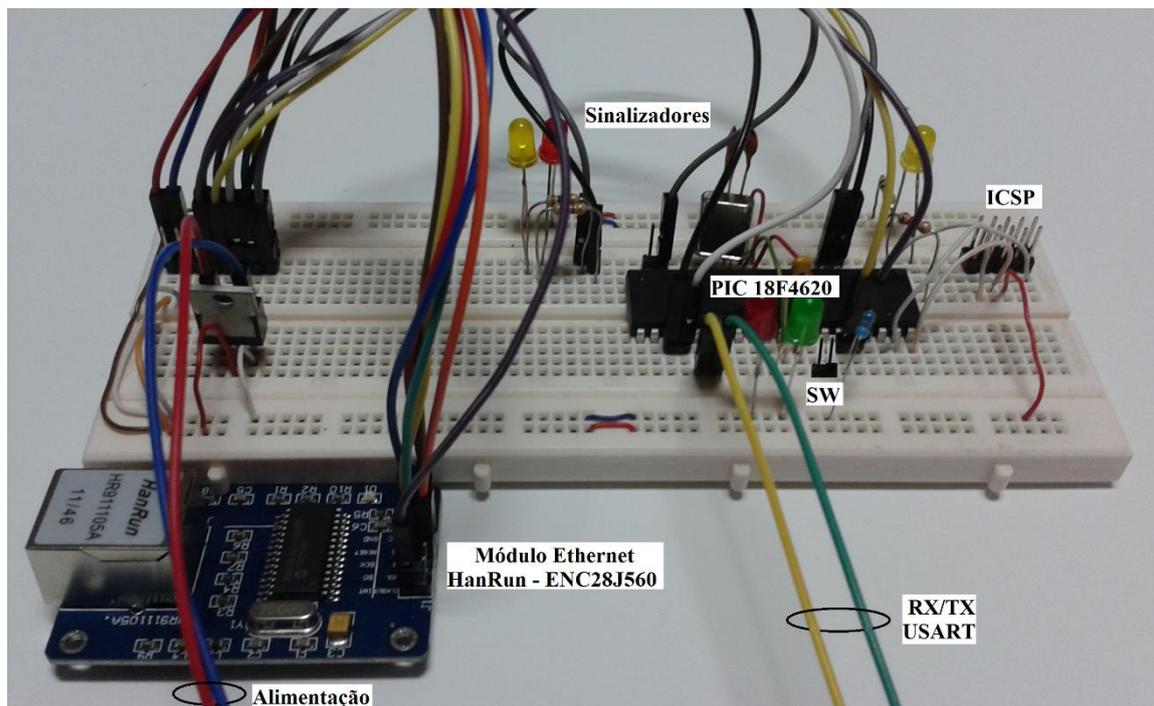
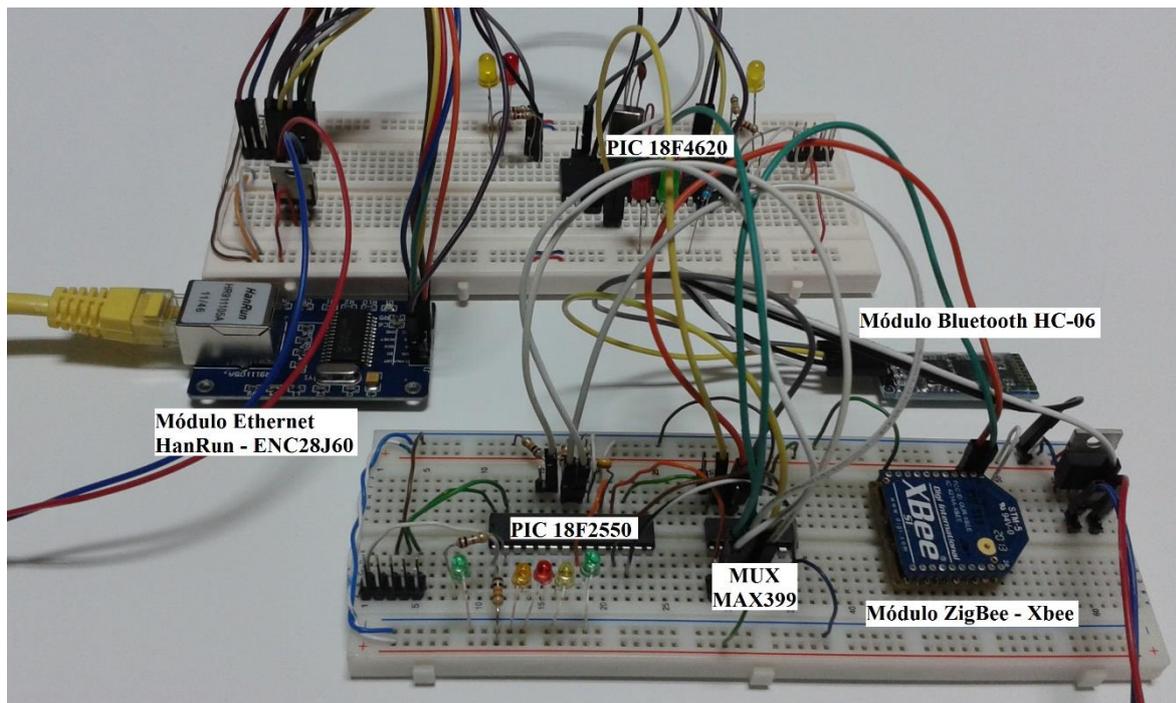


Figura 38 Montagem do Circuito Elétrico do Módulo Central – Circuito Ethernet

A interligação das duas montagens apresentadas aparece ilustrado na Figura 39, facilmente se compreende a dimensão do circuito, o que levou a separação de dois circuitos e montagens isoladas.

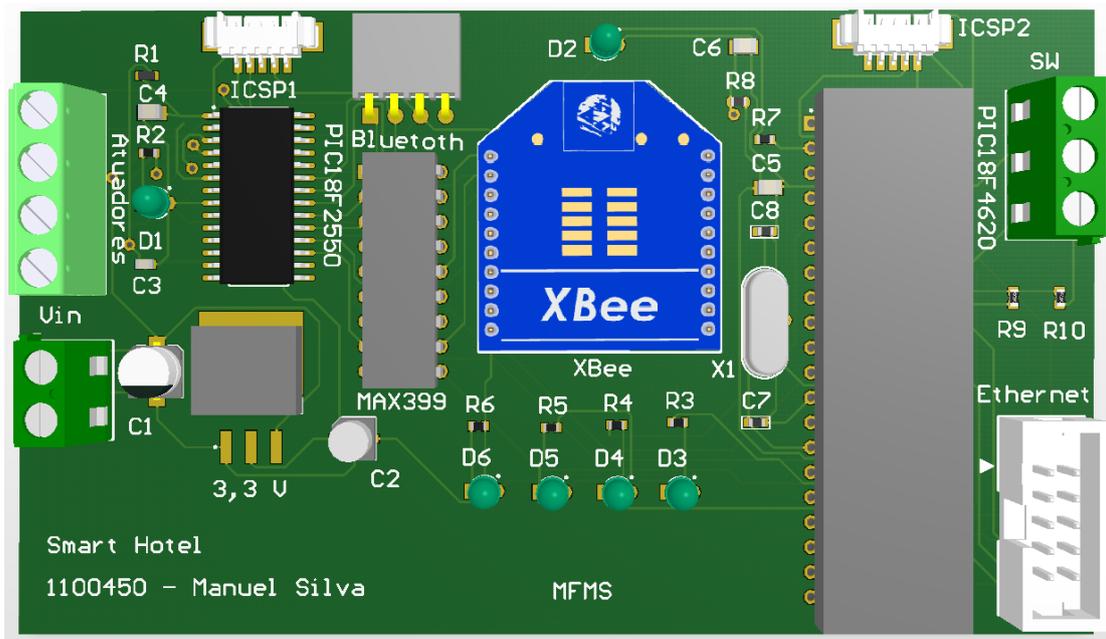


**Figura 39 Montagem Total do Circuito Elétrico do Módulo Central**

Para a realização de todo o módulo foram necessários inúmeros testes unitários e globais da solução desenvolvida, de forma a garantir o funcionamento individual de cada componente e o funcionamento global do módulo central. Seguidamente será referido os principais testes efetuados, esta descrição será dividida em testes dos circuitos central e Ethernet.

- Circuito Elétrico Central:
  - Comunicação XBee com o Módulo Fechadura;
  - Controlo dos canais do multiplexer;
  - Serviços de interrupções externas;
  - Receção de dados dos diferentes módulos de comunicação.
- Circuito Elétrico Ethernet:
  - Comunicação com Servidor Ethernet;
  - Leitura e Envio de dados entre os microcontroladores;

De acordo com a documentação realizada no módulo da fechadura, neste ponto também será explicado a prototipagem do módulo central. Ao longo da documentação deste módulo os circuitos elétricos foram sempre divididos devido a sua dimensão, contudo na realização do protótipo o módulo foi todo desenhado na mesma placa. Na Figura 40 aparece ilustrado a placa de circuito impresso desenvolvida para o módulo central, contudo o Anexo B disponibiliza diferentes perspectivas de visualização da placa.



**Figura 40** Montagem do módulo Central em PCB

A placa desenvolvida será um módulo de quatro elétrico (módulo para calha DIN (*Deutsches Industrie Norm*)), assim torna mais fácil a instalação no quarto, ou seja, todos os periféricos do quarto (TV, A/C, Estores, Iluminação) estão ligados ao quadro elétrico e também torna mais fácil a alimentação do módulo, a ligação á Ethernet também será simples pois tipicamente o *Router* fica instalado na zona técnica do quarto.

Na PCB apresentada estão visíveis parte dos componentes e os conetores de ligações externas, o módulo de Bluetooth e o controlador Ethernet são dois dos módulos de comunicação utilizados e que apenas estão representados na PCB por os conetores respetivos, isto deve-se ao fato de se tratar de placas externas. O módulo Bluetooth (HC-06) permite ser encaixado diretamente no conetor Bluetooth, o controlador Ethernet (ENC28J60) deve ser ligado por um cabo elétrico ao conetor Ethernet. Por ultimo o módulo XBee fica soldado diretamente na PCB.

A placa possui outros conectores com diferentes funcionalidades, os conectores de programação ISCP (1/2) são os conectores utilizados para a programação dos dois microcontroladores presentes na placa, o conector SW (*Swicthes*) trata-se de um conector de duas entradas digitais utilizadas para ligar *switch* da janela e da porta de entrada. O conector Atuadores é o conector de saídas digitais para o controlo dos periféricos do quarto, estas saídas devem ser conectadas aos circuitos de potência, apresentados anteriormente, de forma a permitir o controlo de cargas AC (*Alternating Current*) com impulsos digitais.

A placa é alimentada pelo conector Vin, como já referido, o módulo central será instalado no quadro elétrico, por essa razão a alimentação do módulo deve ser realizado com recurso a uma fonte de alimentação para calha DIN, na Figura 41 está ilustrada uma fonte de alimentação que pode ser utilizada para alimentação do módulo central, esta fonte é ligada diretamente a tensão alternada e dispõem de uma tensão de saída de 5 V contínuos, possibilitando a ligação direta desta fonte á placa.



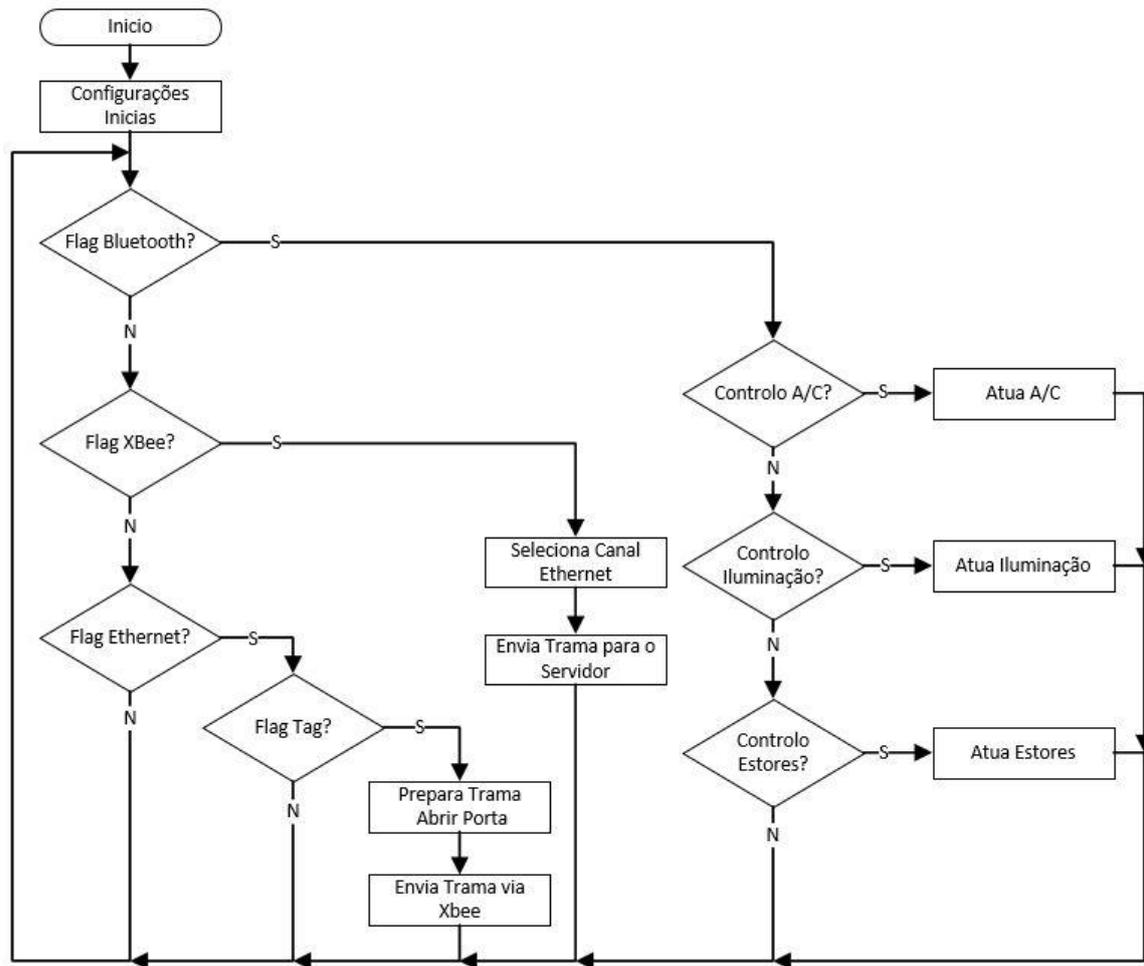
**Figura 41** Fonte de Alimentação para calha DIN, adaptado de [31]

#### 4.2.2. SOFTWARE

No seguimento da explicação *hardware* desenvolvido, será apresentado e explicada o *software* desenvolvido para os microcontroladores do deste módulo. De forma a demonstrar o funcionamento do *software*, a explicação vai ser dividida no fluxograma do programa principal e fluxograma do serviço de interrupções de cada microcontrolador.

O fluxograma ilustrado na Figura 42 representa o funcionamento do programa principal do microcontrolador responsável pelo controlo das comunicações dos diferentes módulos (XBee, Bluetooth e Ethernet). O *software* desenvolvido para este microcontrolador faz o

controlo dos canais do multiplexer de forma a garantir o envio e receção de dados entre os módulos de comunicação corretos.



**Figura 42 Fluxograma do programa principal do PIC 18F2550**

O programa desenvolvido para este microcontrolador, como todos os outros, começa pela definição e inclusão das bibliotecas *standard* necessárias, assim como, a declaração das variáveis do programa. O programa principal do microcontrolador PIC 18F2550, faz o processamento da informação dos diferentes módulos (XBee, Bluetooth e Ethernet) e de seguida faz o seu processamento. A identificação de que módulo está a chegar informação é feita no serviço de interrupções externas que será abordado mais a frente neste capítulo, com a identificação previa da fonte de informação torna-se mais fácil e rápido o seu processamento.

A comunicação do módulo *Bluetooth* com o microcontrolador funciona de forma independente das outras comunicações presentes, ou seja, a aplicação mobile envia

informação por Bluetooth para o controlo dos periféricos existentes no interior do quarto, o microcontrolador mediante os dados recebidos, faz a atuação dos respetivos periféricos, esta comunicação não está dependente das restantes para fechar o ciclo de comunicação.

A comunicação do módulo XBee e do módulo Ethernet, estão diretamente relacionadas, pela sua dependência, ou seja, o microcontrolador recebe dados do módulo XBee referente a tag lida na fechadura, esta informação tem de ser enviada para o módulo Ethernet de forma a ser validada para permitir o acesso ao quarto. A recepção da informação é feita no serviço de interrupção da USART, o programa principal quando tem indicação que chegou informação do XBee, seleciona o canal do módulo Ethernet no multiplexer e envia de seguida a informação recebida para esse módulo, contudo essa informação pode também ser validada com dados guardados em memória, que são periodicamente atualizados pelo servidor. Por sua vez, esse módulo (Ethernet) faz o tratamento e validação dessa informação e devolve a este microcontrolador a resposta de autorização ou não para a abertura da porta, após a recepção da resposta o microcontrolador envia essa informação para o módulo da fechadura pelo canal do XBee caso a resposta seja positiva de abertura.

Como já mencionado, toda a informação recebida na USART dos vários canais do multiplexer é feita no serviço de interrupção para a recepção de dados pela USART. O algoritmo desenvolvido neste serviço de interrupção está ilustrado na Figura 43, esta dividido por recepção de dados de cada módulo, de forma a separar a informação recebida por cada módulo.

A recepção de dados do XBee é igual á do módulo da fechadura, o algoritmo é igual e já explicado anteriormente. Para as tramas de dados das comunicações Bluetooth e Ethernet foi definido um tamanho de 12 *bytes*, desta forma a recepção de dados destes dois módulos é semelhante. A trama é composta por um *start byte* e os restantes *bytes* são dados inerentes as comunicações.

Assim sendo, sempre que é recebido o primeiro *byte* dados de algum destes módulos, este é guardado e validado, caso seja o *start byte* inicia-se o processo de registo da trama de dados recebida, ate que seja detetado o ultimo *byte*. Este processo de validação do *start byte* foi implementado de forma a garantir a qualidade de dados recebido através do multiplexer, isto permite que quando houver atraso na comutação de canal e caso seja perdido o *start byte*, os

dados recebidos serão descartados até que esse *byte* seja recebido. Após recebido esse *byte* todos os dados recebido são registrados numa *string* até ser detectado o fim da trama.

Embora a comutação de canal do multiplexer seja muito rápida, como já referido anteriormente, a necessidade da implementação deste procedimento deve-se ao fato de durante os testes realizados com a montagem final do circuito, terem sido perdidos pontualmente alguns dados entre o microcontrolador e os módulos de comunicação.

Para além da receção de dados por interrupção, foi também utilizado o serviço de interrupções externas, devido á dimensão do algoritmo desenvolvido na interrupção para os dois serviços, os fluxogramas foram separados para facilitar a sua apresentação. O fluxograma da interrupção externa aparece ilustrado na Figura 44. A utilização deste serviço de interrupções é para que seja possível haver comunicações entre o microcontrolador e os módulos de comunicação nos dois sentidos, ou seja, quando o microcontrolador necessita de enviar dados para algum dos módulos de comunicação basta previamente comutar para canal pretendido do multiplexer e em seguida iniciar o envio dos dados. No cenário contrário, o microcontrolador deve ter a indicação de que módulo são enviados os dados, pois para que a receção dos dados seja possível, o canal do multiplexer deve estar comutado para o módulo que iniciar a comunicação.

Para este desenvolvimento foram utilizadas três interrupções externas, uma para cada módulo de comunicação. Quando é ativa alguma das interrupções é comutado de imediato para o canal do multiplexer correspondente à interrupção, de forma a que os dados sejam logo encaminhados pelo o multiplexer até à USART. De seguida é ativa uma flag de indicação de qual módulo foram enviados os dados, esta *flag* é utilizado no algoritmo do programa principal do microcontrolador e na receção de dados da USART por interrupção. Este procedimento é igual para a todas as interrupções externas.

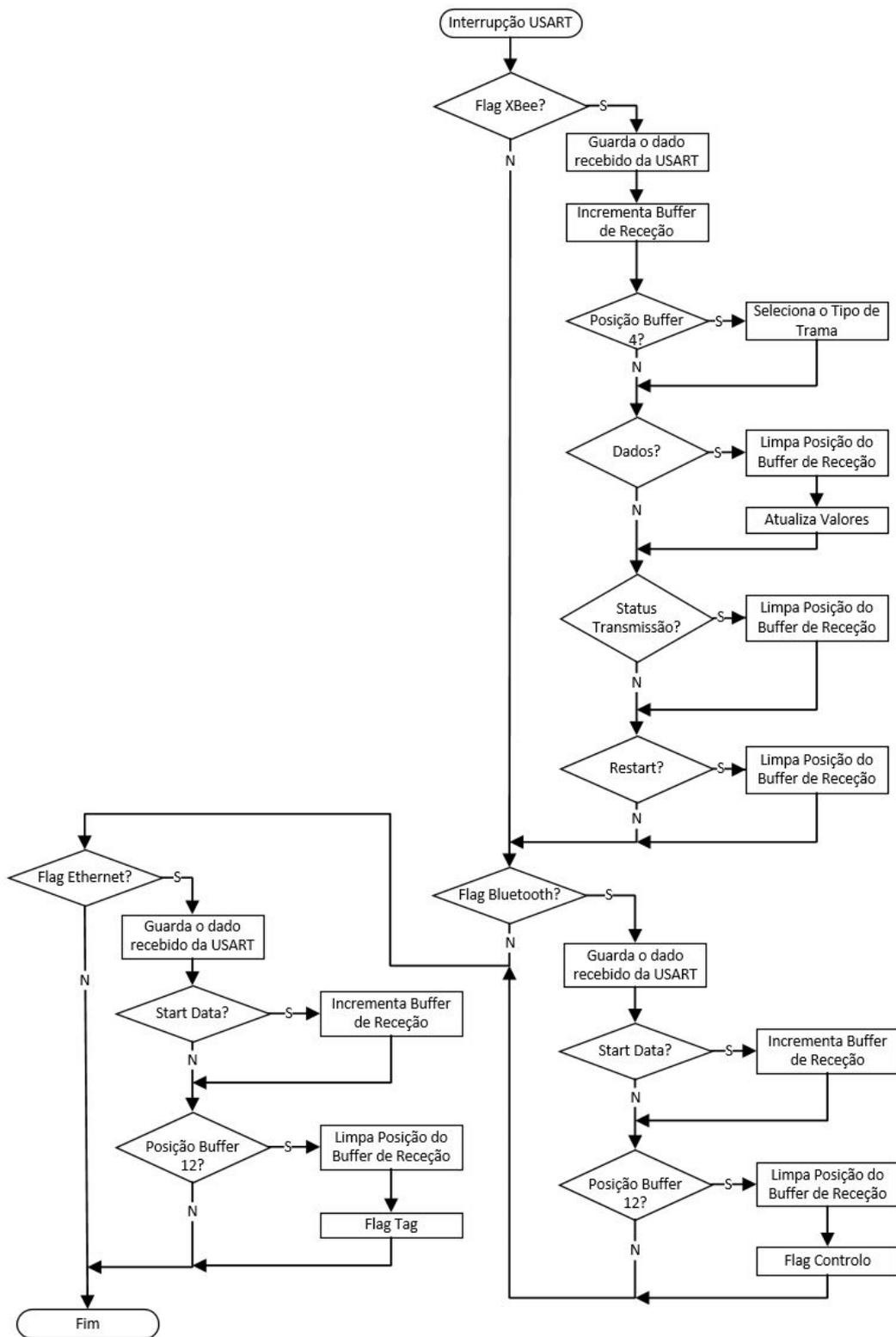
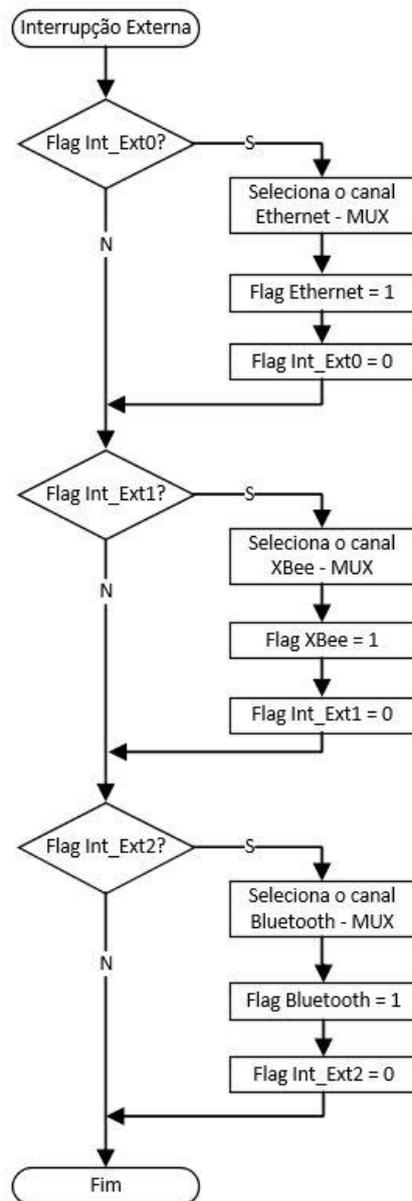


Figura 43 Fluxograma do Serviço de Interrupção da USART PIC 18F2550



**Figura 44 Fluxograma do serviço das interrupções externas PIC 18F2550**

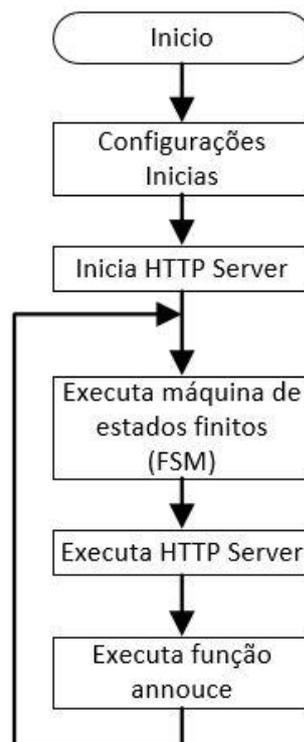
Terminada a explicação do *software* desenvolvido para o microcontrolador PIC 18F2550, será de seguida abordado o *software* referente ao outro microcontrolador do módulo central, o PIC 18F4620. Como já referido anteriormente, este microcontrolador está completamente dedicado a comunicação Ethernet, principalmente para demonstrar a comunicação com a placa Ethernet HanRun.

O projeto que é objetivo deste relatório, deve ser capaz de comunicar com um servidor *web* Ethernet e uma aplicação mobile por Bluetooth que são dois projetos desenvolvidos por outros alunos, ora o cumprimento dos objetivos deste projeto em questão passa por comprovar o funcionamento destas comunicações. A comunicação Bluetooth foi testada e

comprovado através de uma aplicação *mobile free*, nesta aplicação foram recebidas tramas de dados enviados do microcontrolador e posteriormente enviados tramas de dados para o microcontrolador.

A comunicação Ethernet foi comprovada com recurso á montagem do um servidor *web* (HTTP – *Hypertext Transfer Protocol*) básico no microcontrolador utilizando a *stack* TCP/IP da Microchip. O *web server* implementado foi adaptado da referência documental [32]. A referência indicada disponibiliza o código fonte do exemplo, no qual este foi utilizado e adaptado para a aplicação em questão, o microcontrolador utilizado neste exemplo vai de encontro a necessidade da memória necessária para a compilação da *stack* TCP/IP.

Assim sendo, na Figura 45 aparece ilustrado o fluxograma do programa principal do microcontrolador PIC 18F4620.



**Figura 45 Fluxograma do programa principal PIC 18F4620**

O programa começa pelas configurações e declarações iniciais e de seguida inicia o servidor HTTP, que é executado no arranque do microcontrolador, em paralelo com o servidor HTTP, o programa principal também implementa duas funções, HTTPGetVar () e HTTPExecCmd () que fornecem comando e permitem a substituição de variáveis para as páginas dinamicas.

Depois o programa executa três processo ciclicamente, executa a *stack* FSM (*Finite State Machine*) que verifica a existência de novos pacotes e encaminha-os para os componentes da pilha apropriados. Esta função deve ser chamada periodicamente para garantir respostas atempadas, a função faz parte do módulo *stack task* que inicializa e implementa uma máquina de estados finitos para facilitar a multitarefa cooperativa e o protocolo Demux. De seguida o programa executa o servidor HTTP, que irá abrir as conexões HTTP para serem servidas, isto permite navegar através de cada conexão e lidar com a conexão estabelecida, se uma conexão não está terminada, não processa mais nenhuma conexão. Esta função executa a sua tarefa de forma cooperativa, o programa principal chama repetidamente esta função para assegurar todas as ligações abertas ou novas.

Por último executar a função “*announce*”, esta função é chamada após o arranque na altura em que seja detetada a mudança de IP, esta função envia pacotes de difusão UDP (*User Datagram Protocol*) para a porta “*announce*” (30303, por defeito) com informação sobre o dispositivo local NetBios tal como é definido o endereço MAC. Esta função faz parte do módulo que deteta um dispositivo na rede que implemente a *stack* TCP/IP da Microchip, para além desta função o módulo implementa a função *DiscoveryTask* () que implementa um servidor UD simples que escuta a porta “*announce*” para as transmissões que incluem uma mensagem de solicitação. No microcontrolador que está programada a *stack* TCP/IP, proporciona um modelo de multitarefa, isto é dividir a aplicação em módulos e executa-los em *loop* no programa principal do microcontrolador.

Este microcontrolador comunica com o PIC 18F2550 através da USART, esta comunicação é realizada através do serviço de interrupção da USART. Na Figura 46 aparece ilustrado o algoritmo do programa desenvolvido no serviço de interrupção.



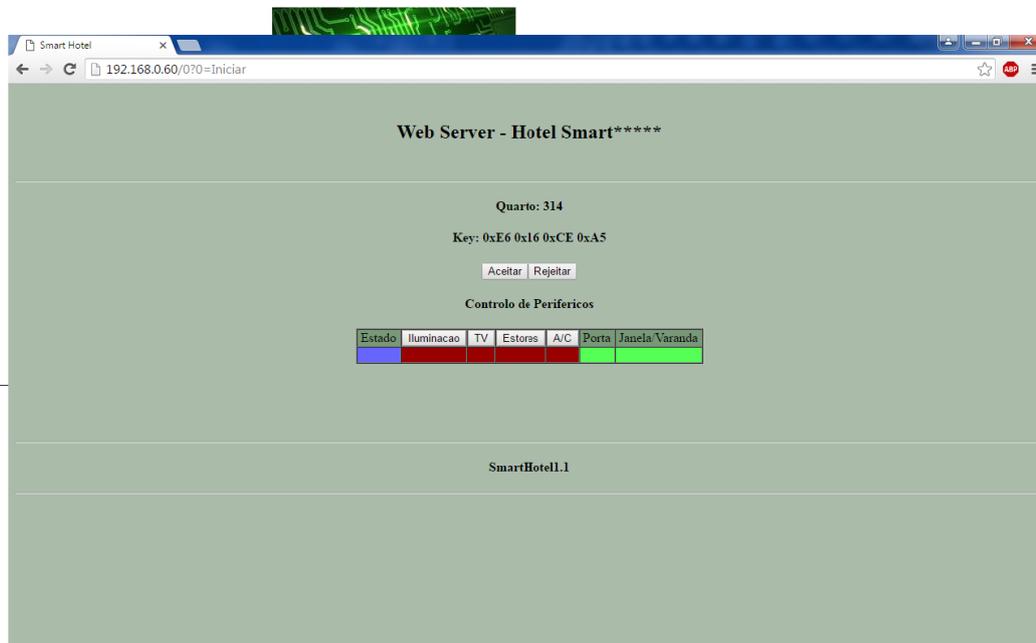
**Figura 46 Fluxograma do serviço de interrupção PIC 18F4620**

O processo de receção de dados pela USART é em tudo igual ao procedimento explicado e implementado no PIC 18F2550 para a recção de dados do Bluetooth e da Ethernet. As tramas de dados são formadas por 12 bytes, aqui também é validado o *start byte* de forma a garantir que esta a receber s trama desde do inicio, valida também o fim da trama.

Como já referido anteriormente, foi desenvolvido um *web server* de forma a demonstrar e garantir o pleno funcionamento do módulo central, permitindo assim garantir que todos os objetivos definidos para este módulo fossem cumpridos. O *web server* desenvolvido está ilustrado na Figura 47.



## Desenvolvimento de Sistema para Controlo de um Quarto de Hotel

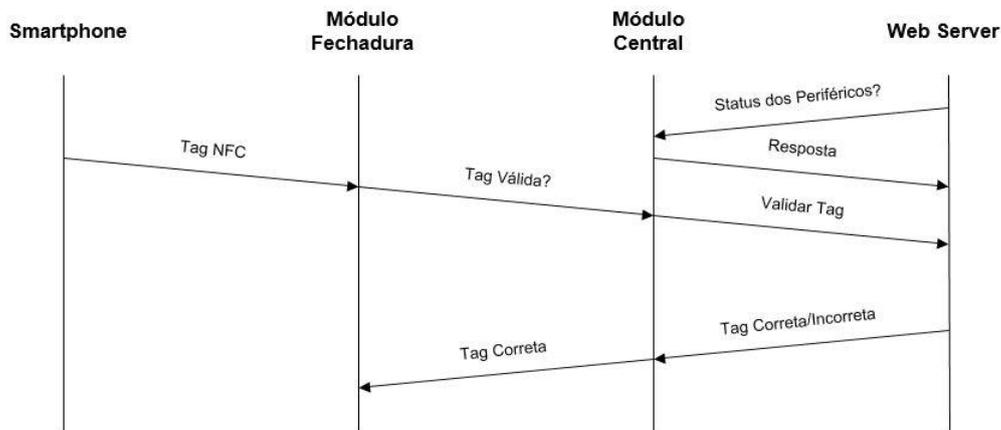


**Figura 47 Web server – Smart Hotel**

Ao *web server* chega a informação da tag NFC que é lida no módulo da fechadura, através daqui é possível permitir o acesso ao quarto ou então negar o acesso, atualmente esta validação é realizada manualmente de forma a validar e comprovar o funcionamento do projeto, futuramente esta validação é realizada automaticamente com recurso a uma base de dados que regista as tag que podem aceder a cada quarto. O *web server* dispõem também da informação de qual os periféricos que estão ligados no momento no quarto e também se a porta de entrada e a janela estão abertas ou fechadas. No caso dos periféricos, estes podem ser desligados remotamente através do *web server*. Esta informação permite desenvolver alguns pontos interessantes para a gestão do hotel, no qual serão referidos mais a frente na referência aos trabalhos futuros.

Na conclusão deste capítulo, após terem sido apresentadas as várias fases de desenvolvimento dos dois módulos deste projeto, será abordada de uma forma geral as comunicações presentes em todo o projeto, pois o *core* deste projeto é a gestão de todas as comunicações existentes nos módulos.

Nesse sentido, a Figura 48 está ilustrado o fluxo geral de comunicações do projeto desenvolvido, no qual é pretendido apresentar o processo de comunicação implementado de forma a permitir o acesso ao quarto de hotel.



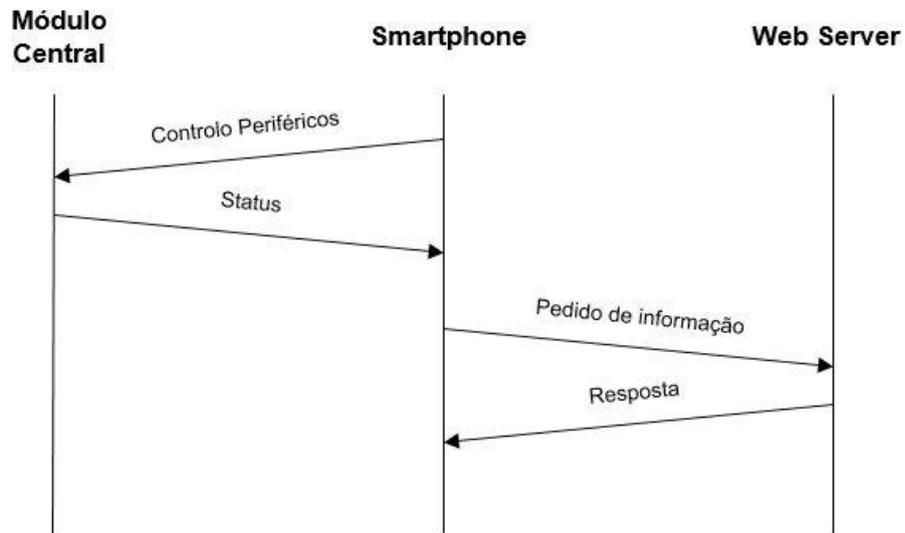
**Figura 48 Fluxo Geral de Comunicação**

O fluxo de comunicação apresenta quatro pontos principais e de referencia que caracterizam este trabalho, sendo eles o *smartphone*, o módulo da fechadura, o módulo central e por ultimo o *web server* do hotel. O *tag NFC* do *smartphone* é lida por rádio frequência pelo leitor NFC do módulo da fechadura, esta informação é recebida pelo microcontrolador através do barramento SPI, de seguida está informação é processada e enviada para o módulo central para a tag de forma a autorizar o acesso ao quarto, esta comunicação é feita entre os dois Xbee presentes um cada módulo.

O microcontrolador central recebe a informação e envia-a para o microcontrolador Ethernet, este por sua vez faz a validação no *web server* através do controlador Ethernet ENC28J60, quando o *web server* responde a informação é devolvida ao módulo central, que em caso de ser ter sido dada a autorização de acesso a informação é enviada ao microcontrolador da fechadura, de forma a permitir a abertura da porta.

Falta ainda referir que pode existir comunicação entre o *web server* e o microcontrolador de Ethernet (módulo central) de forma a fazer leituras relevantes para a gestão do hotel, como por exemplo, informação do estado da porta e das janelas do quarto em situações que o hóspede está ausente ou então numa situação em que esteja a chover e por alguma razão as janelas estejam abertas, permitindo assim lançar alertas para o fecho das mesmas.

Na Figura 49, aparece ilustrado as comunicações que podem ocorrer ao a partir do *smartphone*, a comunicação no interior do quarto de hotel com o módulo central e a comunicação com o *web server* do hotel.



**Figura 49 Fluxo de Comunicação do Smartphone**

O *smartphone* comunica também diretamente com o microcontrolador do módulo Central através do Bluetooth, esta comunicação tem como objetivo o controlo dos periféricos do interior do quarto, esta comunicação também pode ocorrer do módulo Central para o *smartphone* com informação de *status* dos periféricos, por exemplo. Por último o *smartphone* através da *wi-fi* pode aceder diretamente ao *web server* para consulta de informação referente á estadia no hotel.

# 5. CONCLUSÕES

Ao longo do trabalho desenvolvido foram apresentadas todas as fases, planeamento, desenvolvimento e validação da solução (através da montagem em placa de teste), com recurso a montagem de cada módulo. O objetivo principal deste trabalho assenta no controlo de um quarto de hotel, desde controlo de acesso como o controlo dos periféricos do interior do quarto.

O sistema desenvolvido responde aos objetivos iniciais propostos, o sistema constituído por dois módulos no qual funcionam em plena sintonia, o módulo da fechadura faz o controlo de acesso e para isso comunica com o módulo central de forma a validar o acesso corretamente. Por sua vez o módulo central, comunica por Ethernet com o *Web Server* do hotel, comunica também por Bluetooth com um dispositivo móvel, permitindo o controlo dos periféricos do quarto. Este sistema tem como principal ferramenta de funcionamento o *smartphone* tornando o sistema inovador.

Na fase inicial, houve algumas dificuldades relacionadas com a investigação e desenvolvimento dos protocolos de comunicação de cada módulo presente no trabalho (NFC, ZigBee, Bluetooth e Ethernet), contudo o ponto mais crítico foi a comunicação SPI com o módulo NFC. Ao longo do desenvolvimento, a gestão de todas as comunicações presentes no módulo central levou ao desenvolvimento de um circuito externo ao microcontrolador, de forma a auxiliar a correta gestão das comunicações, este desenvolvimento necessitou de mais tempo, pois foi necessário analisar ao detalhe as comunicações em cada um dos canais do multiplexer utilizado.

Na fase de interligação geral dos módulos, ou seja, ligação do módulo da fechadura e do módulo central, foram levantadas algumas questões que foram afinadas com recurso ao *software* de cada microcontrolador.

De um modo geral, a solução desenvolvida quando comparada com os sistemas de controlo de quartos de hotéis atuais, torna-se muito interessante e fácil de implementar em qualquer hotel.

## 5.1. TRABALHOS FUTUROS

Ao longo da elaboração do relatório, foram referidos pequenos pontos como trabalhos futuros, ou seja, algumas sugestões de evolução da solução apresentada. Nesse sentido serve esta secção para apresentar e referir de uma forma breve todos os pontos de melhorias que foram surgindo no decorrer da elaboração do projeto.

O primeiro ponto que pode ser considerado é a leitura do *switchs* presentes no módulo central ligados ao microprocessador da Ethernet, este ponto já foi referido, contudo consiste na leitura destes sensores periodicamente e detetar o seu estado de forma a prevenir situações indesejadas, como por exemplo, detetar a porta do quarto ou a janela aberta, quando for deixada aberta pelo hóspede acidentalmente, pode também o sistema dar alertas se alguma janela do hotel estiver aberta quando estiver a chover ou quando chegar o fim do dia, desta forma o *staff* do hotel pode agir preventivamente sem causar danos de maior.

Um ponto de evolução que deve ser referido é a monitorização dos consumos de energia de cada hóspede no quarto. Uma vez que os periféricos do quarto são controlados pelo *smartphone* através do módulo central, torna-se possível medir o tempo de funcionamento de cada periférico e dessa forma calcular o seu consumo. Com esta informação o sistema do hotel poderá adotar um sistema de descontos com o objetivo de ser competitivo, de acordo com os consumos de cada cliente, assim um cliente com um consumo baixo de energia beneficiava de um maior desconto que um cliente com grandes consumos.

Por fim uma ultima nota é no sentido de o controlo de todos os periféricos evoluir para um controlo pelo *web server* através do *smartphone*, onde seria possível previamente antes da chegada do hóspede ao quarto definir qual a temperatura desejada de forma a aumentar o seu conforto.

## Referências Documentais

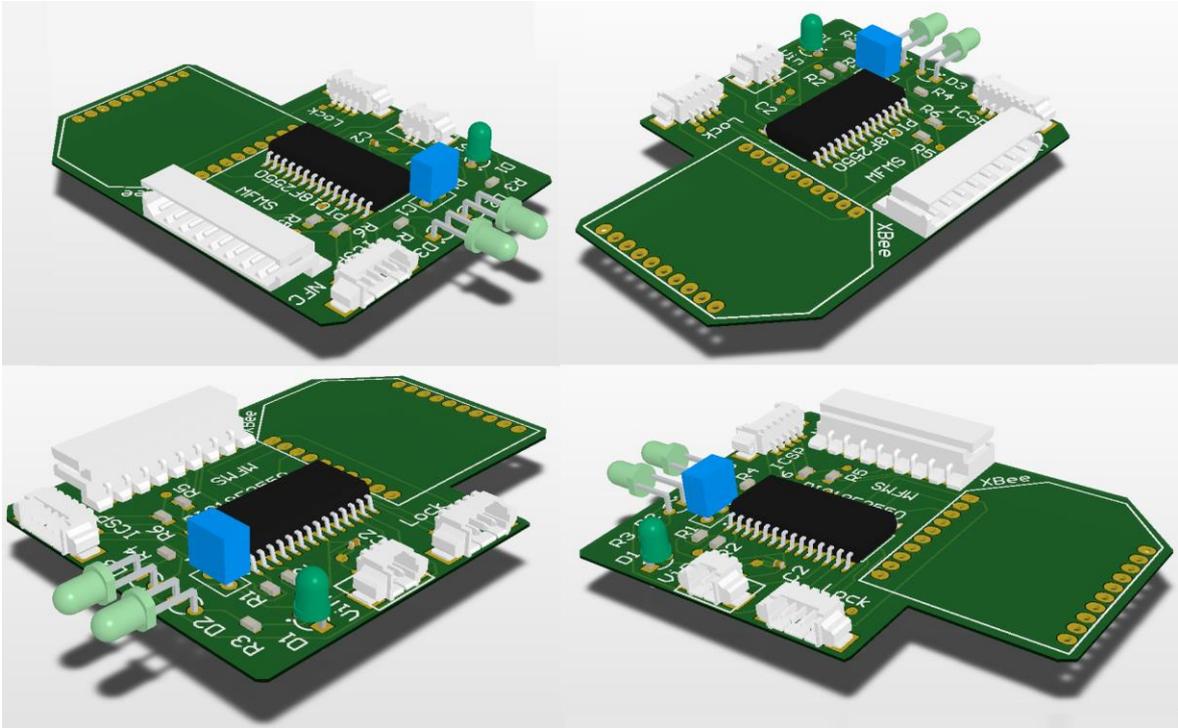
- [1] Luis Antunes – Identificação de Pessoas numa Portaria Virtual. [Consult. 25-03-2015]. Disponível em: <http://repositorio.ipl.pt/bitstream/10400.21/2405/1/Disserta%C3%A7%C3%A3o.pdf>
- [2] Denise Carla A. Zeindin – A Tecnologia do Futuro Wi-Fi (*Wireless Fidelitu*). [Consult. 25-03-2015]. Disponível em: [http://www.inf.furb.br/~zamba/artigos/Artigo\\_Wireless\\_Uni plac\\_2003\\_V1.pdf](http://www.inf.furb.br/~zamba/artigos/Artigo_Wireless_Uni plac_2003_V1.pdf)
- [3] Rodrigo Salvo - Wireless – WLAN Introdução. [Consult. 25-03-2015]. Disponível em: <http://www.ti-redes.com/wireless/wlan-intro/>
- [4] Susanita Inocencio – Calidad de Servicio em Redes Móviles Y Su Aplicación. [Consult. 25-03-2015]. Disponível em: <http://slideplayer.es/slide/1056284/>
- [5] Amadeu Fernandes – Wireless Teams: Comparação de Tecnologia Sem Fios em Equipas de Robôs Móveis. [Consult. 25-03-2015]. Disponível em: <http://books.google.pt/books?id=FCVSAgAAQBAJ&printsec=frontcover#v=onepage&q&f=false>
- [6] André silva – Módulos de Comunicação Wireless para Sensores. [Consult. 25-03-2015]. Disponível em: <http://paginas.fe.up.pt/~ee02055/RelatorioTEC15.pdf>
- [7] HP – Qual a Diferença entre WLAN e WWAN? [Consult. 25-03-2015]. Disponível em: <http://www8.hp.com/h30458/br/ptb/smb/927431.html>
- [8] FEUP – Porquê ZigBee? [Consult. 25-03-2015]. Disponível em: [http://paginas.fe.up.pt/~ee02055/Relatorio\\_ZigBee\\_Hardware.pdf](http://paginas.fe.up.pt/~ee02055/Relatorio_ZigBee_Hardware.pdf)
- [9] Manuela Lima – ZigBee. [Consult. 25-03-2015]. Disponível em: [http://www.gta.ufrj.br/grad/10\\_1/zigbee/padrao.html](http://www.gta.ufrj.br/grad/10_1/zigbee/padrao.html)
- [10] Mário Saleiro – ZigBee – Uma abordagem Prática. [Consult. 25-03-2015]. Disponível em: [http://lusorobotica.com/ficheiros/Introducao\\_ao\\_Zigbee\\_-\\_por\\_msaleiro.pdf](http://lusorobotica.com/ficheiros/Introducao_ao_Zigbee_-_por_msaleiro.pdf)
- [11] Amadeu Fernandes – Comunicação Ad Hoc em Equipas de Robôs Móveis Utilizando Tecnologia ZigBee. [Consult. 25-03-2015]. Disponível em: [http://ap.isr.uc.pt/archive/2012\\_09\\_Tese\\_Mestrado\\_AFernandes.pdf](http://ap.isr.uc.pt/archive/2012_09_Tese_Mestrado_AFernandes.pdf)
- [12] ZigBee Alliance – Application Level standardization. [Consult. 25-03-2015]. Disponível em: <http://www.zigbee.org/zigbee-for-developers/applicationstandards/>
- [13] José Pinheiro – As Redes com ZigBee. [Consult. 25-03-2015]. Disponível em: [http://www.projetoderedes.com.br/artigos/artigo\\_zigbee.php](http://www.projetoderedes.com.br/artigos/artigo_zigbee.php)
- [14] Ober – Is Xbee ZigBee? [Consult. 25-03-2015]. Disponível em: <http://tutorial.cytron.com.my/2011/03/06/is-xbee-zigbee/>

- [15] António Messias – Controle remoto e aquisição de dados via Xbee/ZigBee (IEEE 802.15.4). [Consult. 25-03-2015]. Disponível em:  
<http://www.rogercom.com/ZigBee/ZigBee.htm>
- [16] INFO Wester– Tecnologia Bluetooth: o que é e como funciona? [Consult. 21-09-2016]. Disponível em: <http://www.infowester.com/bluetooth.php>
- [17] André Castro – Redes de Sensores sem fio. [Consult. 25-03-2015]. Disponível em:  
[http://www.gta.ufrj.br/grad/10\\_1/rssf/index.html](http://www.gta.ufrj.br/grad/10_1/rssf/index.html)
- [18] Thiago Siqueira – *Bluetooth* –Características, protocolos e funcionamento. [Consult. 25-03-2015]. Disponível em:  
<http://www.ic.unicamp.br/~ducatte/mo401/1s2006/T2/057642-T.pdf>
- [19] Paulo Stein – Bluetooth. [Consult. 25-03-2015]. Disponível em:  
[http://www.gta.ufrj.br/seminarios/semin2003\\_1/stein/index.html](http://www.gta.ufrj.br/seminarios/semin2003_1/stein/index.html)
- [20] Bob Violino – The History of RFID Technology. [Consult. 27-03-2015]. Disponível em: <http://www.rfidjournal.com/articles/view?1338>
- [21] NFC Forum – NFC Forum specification Architecture. [Consult. Consult. 24-08-2015]. Disponível em: <http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/>
- [22] Sheli McHugh, Kristen Yarney – Near Field Communication: Recent Developments and Library Implications. Hema Ramachandram & Joe Murphy, Series Editors, 2014. [Consult. 24-08-2015]. Disponível na internet:  
 <URL:<https://uwaterloo.ca/renison/sites/ca.renison/files/uploads/files/e-book.pdf>>. ISBN: 9781627054331
- [23] NFC Forum – What it Does. [Consult. Consult. 24-08-2015]. Disponível em:  
<http://nfc-forum.org/what-is-nfc/what-it-does/>
- [24] Ernst Haselsteiner, Klemens BreitfuB - Security in Near Fiel Communication – Strengths and Weaknesses. Autria. Philips Semiconductors. [Consult. 25-08-2015]. Disponível em WWW:  
 <URL:<http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf>>.
- [25] Charles E. Spurgeon, Joann Zimmerman – Ethernet: The Definitive Guide. 2<sup>nd</sup> O’Reilly, 2014. . [Consult. 28-08-2015]. Disponível na internet: <URL:  
<http://www.mvatcybernet.com/IT%20E-BOOKS/IT%20PDF%20Books/IT%20BOOKS/NETWORKING/ETHERNET%20THE%20DEFINITIVE%20GUIDE%202ND%20EDITION.pdf>>. ISBN: 9781449361846
- [26] Adrian Chesney – Introduction to Ethernet. Fieldbus [Consult. 28-08-2015]. Disponível em WWW: <URL: <http://www.ccontrols.com/pdf/ExtV1N3.pdf>>
- [27] Cisco – Cisco Active Network Abstraction Reference Guide, 3.7. [Consult. 28-08-2015]. Disponível em WWW: <URL:  
[http://www.cisco.com/c/en/us/td/docs/net\\_mgmt/active\\_network\\_abstraction/3-7/reference/guide/ANARefGuide37/ethrnt.html](http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37/ethrnt.html)>

- [28] Publituris – Como as novas tecnologias beneficiam os hóspedes e os hotéis. [Consult. 24-06-2016]. Disponível em WWW: <URL: <http://www.publituris.pt/como-as-novas-tecnologias-beneficiam-os-hospedes-e-os-hoteis/>>
- [29] Punto Flotante S.A. - RFID, RC522, SPI module connected to Bolt 18F2550, with visualization of data in mobile smartphone. [Consult. 01-09-2016]. Disponível em www: <URL: <http://www.puntoflotante.net/RFID-MF522-MFRC522-SPI-BLUETOOTH-ENGLISH.htm>>
- [30] Maxim Integrated – Multiplexer Enables Pseudomultidrop RS-232 Transmission. [Consult. 01-09-2016]. Disponível em www: <URL: <https://www.maximintegrated.com/en/app-notes/index.mvp/id/588>>
- [31] FFonseca – Fontes de Alimentação para calha DIN – MDR – Mean Well. [Consult. 01-09-2016]. Disponível em www: <URL: [http://www.ffonseca.com/produto.aspx?lang=pt&id\\_object=484900&name=Fontes-de-alimentacao-para-calha-DIN---MDR---Mean-Well](http://www.ffonseca.com/produto.aspx?lang=pt&id_object=484900&name=Fontes-de-alimentacao-para-calha-DIN---MDR---Mean-Well)>
- [32] HP.Spin – Web Server no PIC18F4620. [Consult. 01-09-2016]. Disponível em www: <URL: <http://www.hpspin.com.br/site1/circuitos/picwebserver/>>
- [33] Microchip – ENC28J60 Data Sheet. [Consult. 21-09-2016]. Disponível em www: <URL: <http://ww1.microchip.com/downloads/en/DeviceDoc/39662c.pdf>>



# Anexo A. PCB – Módulo Fechadura



## Anexo B. PCB – Módulo Central

