**RENATO RAMOS DA SILVA**

# DESENVOLVIMENTO DE UM MÓDULO DE ACIONAMENTO PARA ABERTURA DA FECHADURA DE UM QUARTO DE HOTEL BASEADO NA TECNOLOGIA NFC

**Florianópolis**
**2014**

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA**
**DEPARTAMENTO ACADÊMICO DE ELETRÔNICA**
**CURSO DE PÓS-GRADUAÇÃOEM DESENVOLVIMENTO DE PRODUTOS ELETRÔNICOS**

**RENATO RAMOS DA SILVA**

# DESENVOLVIMENTO DE UM MÓDULO DE ACIONAMENTO PARA ABERTURA DA FECHADURA DE UM QUARTO DE HOTEL BASEADO NA TECNOLOGIA NFC

Trabalho de conclusão de curso submetido à banca examinadora do curso de Pós-Graduação em Desenvolvimento de Produtos Eletrônicos do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, como requisito parcial à obtenção do título de Especialista em Desenvolvimento de Produtos Eletrônicos.

Professor Orientador: Joel Lacerda, Dr. Eng.

**Florianópolis, 2014**

CDD 629.895
S586d

Silva, Renato Ramos da
Desenvolvimento de um módulo de acionamento para abertura da fechadura de um quarto de hotel baseado na tecnologia NFC [MP] / Renato Ramos da Silva; orientação de Joel Lacerda. – Florianópolis, 2014.

1 v.: il.

Monografia de Pós Graduação (Desenvolvimento de Produtos Eletrônicos) – Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Inclui referências.

1. Automação residencial. 2. Tecnologia NFC. 3. Acionamento de fechadura. 4. Hotel. 5. Dispositivos móveis. I. Lacerda, Joel. II. Título.

Sistema de Bibliotecas Integradas do IFSC
Biblioteca Dr. Hercílio Luz – Campus Florianópolis
Catalogado por: Ana Paula F. Rodrigues Pacheco CRB 14/1117

# DESENVOLVIMENTO DE UM MÓDULO DE ACIONAMENTO PARA ABERTURA DA FECHADURA DE UM QUARTO DE HOTEL BASEADO NA TECNOLOGIA NFC

**RENATO RAMOS DA SILVA**

Este trabalho foi julgado adequado para obtenção do Título de Especialista em Desenvolvimento de Produtos Eletrônicos e aprovado na sua forma final pela banca examinadora do Curso de Pós-Graduação em Desenvolvimento de Produtos Eletrônicos do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

Florianópolis, 12 de Setembro de 2014.

Banca Examinadora:

_____

Joel Lacerda, Dr. Eng.
Orientador

_____

Clovis Antônio Petry, Dr. Eng.

_____

Daniel Lohmann, M. Eng.

## RESUMO

A automação residencial e predial vem se destacando ano após ano nos mais variados ramos de atividade e está deixando de ser uma solução futurística para tornar-se um elemento comumente encontrado em residências e estabelecimento comerciais. Segundo o diretor executivo da AURESIDE (Associação Brasileira de Automação Residencial) a quantidade de projetos de automação apresentou um crescimento de 35% desde 2011. Esse crescimento deve-se à redução de custos que a automação proporciona e ao público jovem que está investindo em imóveis e é adepto às novas tecnologias. Nesse contexto estão contidas as fechaduras *hi-tech*, que podem compor tanto uma solução de automação residencial quanto uma comercial como, por exemplo, os hotéis. Considerando a disseminação do uso dos *smartphones* e as facilidades que esses dispositivos oferecem, foi idealizado o conceito de acesso a um determinado estabelecimento através de dispositivos móveis, isentando o usuário de carregar consigo chaves físicas ou cartões de acesso. Este trabalho apresenta o desenvolvimento de um módulo de acionamento de fechadura, mostrando em detalhes a arquitetura da solução, o hardware e *firmware* construídos, visando validar um conceito que futuramente poderá tornar-se um produto comercial.



Palavras-Chave: Automação, Fechadura, Hotel, *Smartphone*.

## ABSTRACT

The residential automation has been highlighted every years in many in various industries and is no longer a futuristic solution to become an element commonly found in residential and commercial property. According to the executive director of Aureside (Brazilian Association of Residential Automation) the amount of automation projects grew by 35% since 2011. This growth is due to the cost reduction that provides automation and younger audience that are investing in houses and are adept to new technologies. In this context are the high-tech locks, that can comprise either a solution of a commercial home automation as, for example, hotels. Considering the widespread use of smartphones and the facilities that these devices offer, was conceived the concept of access to a particular property via mobile devices, freeing the user to carry around physical keys or access cards. This research presents the development of a trigger module lock, the solution architecture, the hardware and firmware built with the objective of validating a concept that may eventually become a commercial product.

Key-Words: Automation, Lock, Hotel, Smartphone.

## LISTA DE FIGURAS

Figura 1 - Painel tátil TEV2 ..... 18
Figura 2 - Fechadura com biometria e senha ..... 26
Figura 3 - Fechadura *Lockitron* ..... 26
Figura 4 - Fechadura Okidokeys ..... 27
Figura 5 - Comparativo entre as topologias em estrela e malha 31
Figura 6 - Tag NFC Fonte: UBITAP (2014) ..... 35
Figura 7 – Arduino Duemilanove ..... 37
Figura 8 - Visão geral da solução ..... 38
Figura 9 – Cenário de aplicação ..... 39
Figura 10 - Diagrama de sequência para acesso permitido ..... 44
Figura 11 - Diagrama de sequência para acesso negado ..... 46
Figura 12 - Arquitetura MAF ..... 47
Figura 13 - Esquema elétrico do MAF ..... 49
Figura 14 - Layout da placa protótipo do MAF ..... 50
Figura 15 - Suporte das pilhas AA ..... 51
Figura 16 - Módulo PN532 NFC ..... 52
Figura 17 - Configuração UART do módulo NFC ..... 53
Figura 18 - Módulo *Bluetooth* ..... 54
Figura 19 - Fechadura utilizada no projeto ..... 57
Figura 20 - Fluxograma da solução ..... 59
Figura 21 - Planta baixa do ambiente de testes ..... 61
Figura 22 – Protótipo do MAF ..... 62
Figura 23 - Feedback de não reconhecimento do módulo NFC. 63
Figura 24- App NFC tools no *smartphone* Nexus 5 ..... 64
Figura 25 - Tag genérica NFC ..... 65
Figura 26 - Código ID NFC do cartão genérico ..... 66
Figura 27 - Cartão de acesso NFC ..... 66
Figura 28 - Código ID NFC do cartão de acesso ..... 67
Figura 29 - Pareamento com terminal *Bluetooth* ..... 68
Figura 30 - Leitura do cartão genérico NFC ..... 69
Figura 31 - Envio do código NFC ..... 69
Figura 32 - Retorno de acesso permitido do MCA para o MAF . 70
Figura 33 - Retorno de acesso negado do MCA para o MAF .... 70
Figura 34 - Feedback de acesso permitido ..... 71
Figura 35 - Feedback de acesso negado ..... 71
Figura 36 - Estado stand by ..... 72

## LISTA DE TABELAS

Tabela 1 - Comparativo entre fechaduras ..... 27
Tabela 2 - Classes *Bluetooth* ..... 29
Tabela 3 - Comparativo entre *Bluetooth* e Zigbee ..... 30
Tabela 4 - Requisitos Funcionais ..... 40
Tabela 5 - Requisitos não Funcionais ..... 41
Tabela 6 - Regras de Negócio ..... 41
Tabela 7 - Estado do LED de Interação ..... 56
Tabela 8 - Estados dos Alertas Sonoros ..... 56
Tabela 9 - Lista de materiais para a montagem do protótipo ..... 58
Tabela 10 - Código ID dos cartões NFC ..... 65

## LISTA DE QUADROS

Quadro 1 - Especificações do módulo Bluetooth ..... 54
Quadro 2 - Especificações do Arduino Duemilanove ..... 55

## LISTA DE ABREVIATURAS

| | |
|---|---|
| BLE | *Bluetooth Low Energy* |
| CES | *Consumer Electronics Show* |
| ECMA | *European Computer Manufacturers Association* |
| ETSI | *European Telecommunications Standards Institute* |
| GECAD | Grupo de Investigação em Engenharia do Conhecimento e Apoio à Decisão |
| IDE | *Integrated Development Environment* |
| ISEP | Instituto Superior de Engenharia do Porto |
| ISO | *International Organization for Standardization* |
| LAN | *Local Area Network* |
| LE | *Low Energy* |
| LED | *Light Emitting Diode* |
| PAN | *Personal Area Network* |
| PC | *Personal Computer* |
| PCI | Placa de Circuito Impresso |
| RFID | *Radio Frequency Identification* |
| RGB | *Red / Green / Blue* |
| NFC | *Near Fild Comunication* |
| MAF | Módulo de Acionamento da Fechadura |
| MCA | Módulo de Controle e Acionamento |
| MCU | Microcontrolador |

**RESUMO** ..... **6**

**ABSTRACT** ..... **8**

**LISTA DE FIGURAS** ..... **10**

**LISTA DE QUADROS** ..... **12**

**LISTA DE ABREVIATURAS** ..... **13**

**1 INTRODUÇÃO** ..... **16**

1.1 MOTIVAÇÃO ..... 17

1.2 PROBLEMATIZAÇÃO ..... 18

1.2.1 Solução Proposta ..... 19

1.3 OBJETIVOS ..... 20

1.3.1 Objetivo Geral ..... 20

1.3.2 Objetivos Específicos ..... 20

1.4 METODOLOGIA ..... 21

**2 FUNDAMENTAÇÃO TEÓRICA** ..... **23**

2.1 HOTELARIA ..... 23

2.1.1 Histórico ..... 23

2.1.2 O Início da Hotelaria no Brasil ..... 23

2.1.3 Panorama Atual ..... 24

2.1.4 Fechaduras Modernas ..... 25

2.1.5 Protocolos de Comunicação ..... 28

**3 DESENVOLVIMENTO** ..... **37**

3.1 VISÃO GERAL ..... 38

3.2 COLETA E ANÁLISE DE REQUISITOS ..... 40

3.2.1 Levantamento de Requisitos ..... 40

3.2.2 Regras de Negócio ..... 41
3.2.3 Diagrama de Sequência ..... 43
3.3 ARQUITETURA DO MAF ..... 47
3.3.1 Esquema Elétrico ..... 48
3.3.2 Layout do Protótipo ..... 50
3.3.3 Fonte Interna ..... 51
3.3.4 Regulador de Tensão ..... 51
3.3.5 Módulo NFC ..... 51
3.3.6 Módulo *Bluetooth* ..... 53
3.3.7 Controlador ..... 54
3.3.8 LED de Interação ..... 55
3.3.9 Alertas Sonoros ..... 56
3.3.10 Fechadura ..... 57
3.3.11 Lista de Materiais ..... 57
3.4 *FIRMWARE* DO MAF ..... 58

**4 RESULTADOS ..... 60**
4.1 AMBIENTE DE TESTES ..... 60
4.2 TESTES UNITÁRIOS ..... 62
4.2.1 Reconhecimento do Módulo NFC ..... 63
4.2.2 Leitura do NFC ..... 64
4.2.3 Recebimento da Permissão ..... 70
4.2.4 *Feedbacks* Visuais ..... 72
4.3 TESTES FUNCIONAIS ..... 73

**5 CONCLUSÃO ..... 74**
5.1 TRABALHOS FUTUROS ..... 76

**6 REFERÊNCIAS BIBLIOGRÁFICAS ..... 77**

**APÊNDICES..... 80**

**APÊNDICE A – CHECK-LIST DE TESTES UNITÁRIOS..... 81**

# 1 INTRODUÇÃO

Antes de mencionar a atual situação do mercado hoteleiro e as principais tecnologias hoje empregadas, é preciso mostrar como surgiu essa área a fim de se conhecer sua origem, sua evolução e imaginar o que ainda está por vir nesse ramo de atividade.

O primeiro registro que se tem de uma hospedaria ocorreu na Grécia Antiga durante os jogos olímpicos e esses jogos eram tão importantes na época que interrompiam até mesmo guerras em andamento. Milhares de pessoas deslocavam-se para prestigiar tal evento e com o aumento do número de expectadores fez-se necessária a criação de um alojamento com o intuito de abrigar os visitantes (SERAFIN, 2005).

Diferentemente da Grécia, na Roma antiga o alojamento de pessoas surgiu a partir da expansão do império e assim os funcionários encarregados de transportar as correspondências precisavam dormir em outras cidades para então retornar à Roma ou continuar o trajeto para dar continuidade às entregas das correspondências. Já o Brasil iniciou suas atividades hoteleiras a partir do aumento do número de pessoas que transitavam pela cidade do Rio de Janeiro após a chegada da família real portuguesa, no dia 8 de março de 1808 (SERAFIN, 2005).

A tecnologia vem se destacando dia após dia nas mais variadas áreas e no setor hoteleiro não é diferente. Inúmeras facilidades da domótica foram incorporadas nesse ramo de atividade, porém as chaves e fechaduras sofreram poucas mudanças nesse sentido desde o século XIX. A empresa Assa Abloy, líder no mercado de fabricação de fechaduras, passou a investir cerca de 2,9% do seu faturamento em pesquisa e desenvolvimento, com o intuito de agregar novas funcionalidades nas fechaduras comuns (SCRUTTON, 2013).

Além das fechaduras *key card wireless* existem outros modelos que agregam os mais variados tipos de tecnologias tais como o *Bluetooth*, leitura biométrica, NFC (*Near Field Comunication)* e *Ethernet*. A empresa Portuguesa nControl, comercializa o modelo de fechadura NC F500, que além de realizar o acionamento através da impressão digital, possui um

teclado matricial para a inserção de senhas, dispensando a utilização de uma chave mecânica (NCONTROL, 2014).

Outra fechadura que se destaca por seu diferencial, é um modelo lançado pela empresa americana *Lockitron* que funciona em conjunto com aplicativos, compatíveis com Android ou iOS, e a partir deste é realizada a abertura ou trancamento da fechadura de qualquer lugar do mundo, desde que tenha acesso à internet (LOCKITRON, 2012).

Em janeiro deste ano, durante a *Consumer Electronics Show* (CES) 2014, foi lançada a fechadura Okidokeys. Dotadas de conexão *Bluetooth* 4.0 e NFC, a fechadura permite abrir e/ou fechar uma porta através de aplicativos compatíveis com os sistemas operacionais Android e iOS (SOUZA, 2014).

De acordo com Rajeev Chand, chefe de pesquisa da Rutberg & Co, as chaves passarão a ser um objeto arcaico e se tornarão obsoletas ao passar dos anos (RICHTEL & KOPYTOFF, 2011).

O investimento tecnológico em fechaduras nos últimos anos, o constante crescimento na domótica e a disseminação do uso dos smartphones, é com base nesses panoramas que ocorreu a concepção da solução proposta neste trabalho.

## 1.1 MOTIVAÇÃO

O Instituto Federal de Santa Catarina (IFSC), em parceria com o Instituto Superior de Engenharia do Porto (ISEP), através do programa PROPICIE, disponibilizou a oportunidade de alunos dos cursos técnicos, graduação e pós-graduação participarem de um programa de intercambio voltado para a pesquisa. Tive a honra de ser selecionado para trabalhar em um projeto de automação concebido por professores pesquisadores do ISEP, para a área hoteleira. O projeto estava em fase inicial e não havia qualquer documentação, sendo necessária a realização de um estudo sobre as tecnologias disponíveis com a finalidade de justificar as escolhas, assim como analisar soluções similares que ajudariam na definição do escopo e na escolha dos requisitos.

O sistema de automação hoteleira proposto pela empresa TEV2 possui um controlador central e faz uso de painéis táteis (Figura 1) instalados, individualmente, em cada quarto. Esses

painéis independem uns dos outros e são utilizados como interface do usuário com o sistema de controle podendo, através destes, controlar iluminação, temperatura, persiana, dentre outros recursos do quarto de hotel. Nessa mesma solução o controle de acesso é realizado através de *key card wireless* que utiliza a tecnologia *Radio Fequency Identification* (RFID) (TEV2, 2014).

Figura 1 - Painel tátil TEV2
Fonte: TEV2 (2014)

Segundo a companhia de pesquisa norte americana ABI Research, no ano de 2014 haverá mais de 500 milhões de dispositivos com o NFC presentes no mercado (SCRUTTON, 2013).

Considerando a solução desenvolvida pela empresa TEV2, a disseminação do uso de smartphones em todo o mundo e a alta aplicabilidade do NFC, foi idealizado o conceito de controle centralizado, substituindo os painéis táteis por dispositivos móveis, no qual possibilita realizar a abertura das fechaduras e controlar os recursos de um quarto de hotel, tais como iluminação, temperatura entre outros serviços oferecidos através de um único aparelho.

## 1.2 PROBLEMATIZAÇÃO

A área de automação residencial está em constante crescimento nos últimos anos e segundo AUSERIDE (2014), os

Estados Unidos é o país que possui as soluções mais avançadas no mundo, totalizando 3,5 milhões de sistemas instalados no final de 2012, sendo que 0,7 milhão destes são sistemas integrados de múltiplas funções e 2,8 milhões são soluções projetadas para uma função específica.

Diante das facilidades que a automação proporciona no âmbito residencial, as empresas adaptaram as soluções da domótica e passaram a utilizar essas em seus prédios comerciais e oferecendo serviços baseados na automação dos recursos oferecidos por cada empresa. Nesta linha estão os hóteis, onde é comum encontrar atualmente elevadores que aceitam o comando somente de posse de um cartão, previamente registrado na hora do *check-in* do hotel. Outro exemplo ainda na área hoteleira é a utilização de cartões RFID para abrir as fechaduras e controlar o uso das tomadas e interruptores do quarto. Em ambas as situações os serviços são disponibilizados somente após o cartão ser inserido em um mecanismo próprio para este fim.

Nos dias de hoje é cada vez mais comum projetar e desenvolver uma solução de automação considerando as potencialidades dos *smartphones*, tanto nas atividades rotineiras que antes consumiam um tempo excessivo dos usuários como pagamento de contas, transações bancárias, quanto as mais corriqueiras em um computador pessoal (PC) como troca de e-mails, foram incorporadas aos *smartphones* e o usuário se vê cada vez mais dependente desses dispositivos, uma vez que diferentes empresas oferecem uma gama de serviços os quais o usuário pode usufruir através de um único aparelho.

Diante deste cenário, foi idealizado o desenvolvimento de uma solução para automatizar os serviços de um hotel. Este sistema faz a gestão em tempo real de grande parte dos serviços oferecidos por um hotel, além de permitir ao hóspede gerenciar os recursos disponíveis no quarto tal como televisão, ar condicinado, iluminação e fechadura.

### 1.2.1 Solução Proposta

A solução proposta neste trabalho é uma parte do sistema como um todo, ou seja, foi idealizada uma solução de automação que abrange grande parte dos recursos oferecidos por um hotel e

este projeto mostra o desenvolvimento de um módulo para essa solução.

Seguindo o raciocínio da seção anterior, pode-se dizer que a utilização de *smartphones* é imprescindível para o desenvolvimento e utilização de um sistema de automação e é focado nesses dispositivos que a solução geral é gerida. É proposta a utilização desses dispositivos para controlar e acionar, interna ou externamente, os serviços oferecidos por um hotel seja ele um serviço de quarto, o controle da temperatura, da luminosidade, além de outros recursos incluindo o acesso aos quartos. Este último é foco principal deste trabalho, ou seja, o desenvolvimento de um módulo de acionamento da fechadura, sem fazer uso de técnicas comuns como chaves mecânicas ou cartões RFID. A ideia é realizar o acionamento da fechadura e permitir o acesso aos quartos através de smartphones.

## 1.3 OBJETIVOS

### 1.3.1 Objetivo Geral

O objetivo geral deste trabalho é desenvolver um módulo de *hardware* e *firmware* para acionar a fechadura de um quarto de hotel utilizando, como interface, dispositivos móveis.

### 1.3.2 Objetivos Específicos

A proposta deste projeto é desenvolver um módulo de acionamento capaz de abrir a fechadura de um quarto de hotel utilizando a tecnologia NFC a partir de dispositivos que utilizem o sistema operacional da Google, o Android.

Tendo em vista a afirmação anteriormente citada, seguem os objetivos específicos deste projeto:

- Desenvolver um conceito do módulo de acionamento;
- Definir a tecnologia a ser utilizada para a comunicação entre os módulos de acionamento e controle;
- Desenvolver hardware e firmware do módulo;

- Construir um protótipo para o acionamento da fechadura;
- Testar e avaliar a solução; e
- Documentar os resultados obtidos nos testes.

## 1.4 METODOLOGIA

O desenvolvimento deste trabalho foi dividido em cinco macros etapas, sendo elas: estudo, desenvolvimento, construção, testes e documentação.

Na primeira etapa foi realizado um estudo referente às soluções de automação presente em hotéis, o princípio de acionamento de fechaduras eletrônicas, assim como as tecnologias utilizadas nas áreas de automação residencial e predial. Este estudo foi realizado com base nas documentações e apresentações de empresas que desenvolvem soluções na área, além de artigos, livros e trabalhos correlatos referentes às tecnologias em questão. Ao fim desta etapa foi possível identificar as características dos produtos existentes no mercado, servindo como base para a definição dos requisitos do módulo desenvolvido.

Uma vez conhecida a arquitetura da solução como um todo, na segunda etapa foi definido o escopo do trabalho. Foram decididos os modelos de fechadura e *smartphone*, além das tecnologias e componentes a serem utilizados para a comunicação entre os módulos. As escolhas foram tomadas com base em soluções similares, baixo consumo de energia e nos módulos que o Instituto Superior de Engenharia do Porto (ISEP) possuia.

Em seguida foi elaborado o protótipo da PCI, utilizando o *software* Eagle, e o *firmware* da solução. Após a simulação do protótipo em software, utilizando o software Protheus 8, foi montado o protótipo, ou seja, a utilização de um módulo de desenvolvimento com o *firmware* gravado. Ambos os *softwares* foram escolhidos por serem amplamente utilizados no meio acadêmico e pela gratuidade.

Na etapa de testes, o protótipo desenvolvido na etapa anterior foi submetido, em um ambiente controlado e simulado, à uma sequencia de testes. Para documentar os resultados dessa

etapa, foi elaborado um *check-list* baseado em situações reais visando avaliar o comportamento da solução.

Documentação é a atividade principal da última etapa deste projeto. Durante toda a execução das etapas anteriores, buscou-se registrar grande parte das informações pertinentes ao desenvolvimento do módulo proposto por este trabalho de curso.

# 2 FUNDAMENTAÇÃO TEÓRICA

## 2.1 HOTELARIA

Antes de mencionar a atual situação do mercado hoteleiro e as principais tecnologias hoje empregadas, é preciso mostrar como surgiu essa área, a fim de entender a origem, a evolução e o que ainda está por vir nesse ramo de atividade.

### 2.1.1 Histórico

Na Grécia Antiga os jogos olímpicos duravam dias e eram de extrema importância, capazes de interromper até mesmo guerras em andamento. Devido a essa importância, milhares de pessoas deslocavam-se para prestigiar tal evento e com o aumento do número de expectadores foram criados os balneários e um alojamento, com um tamanho aproximado de dez mil metros quadrados, com o intuito de abrigar os visitantes. Essa hospedaria é o primeiro registro que se tem de um hotel (SERAFIN, 2005).

O conceito de hospedagem só se faz necessário quando há um primeiro deslocamento e é baseado nesse conceito que alguns autores defendem a tese de que o deslocamento do povo Romano é um marco importantíssimo para a criação e desenvolvimento do setor hoteleiro. Durante a expansão do império Romano, foi iniciada a construção de estradas que ligavam Roma às cidades conquistadas e um funcionário Romano era o responsável por transportar as correspondências de uma cidade para outra. À medida que o império foi se expandindo, tornou-se impossível entregar as correspondências e retornar à Roma no mesmo dia, o que acarretou a necessidade de hospedar esses funcionários em lugares particulares ou abandonados (SERAFIN, 2005).

### 2.1.2 O Início da Hotelaria no Brasil

O Rio de Janeiro tornou-se um marco inicial da hotelaria no Brasil junto com a cidade de São Paulo no século XIX, isso ocorreu devido à chegada da corte Portuguesa em 1808, que

ocasionou o aumento do trânsito de estrangeiros pela cidade e assim foi necessário criar locais de hospedagem preparados para acomodar uma quantidade maior de pessoas que ali viviam (ANDRADE, 2000). De lá pra cá muita coisa mudou e o desenvolvimento tecnológico fez com que houvesse uma notável evolução nesse setor.

### 2.1.3 Panorama Atual

A tecnologia vem se destacando dia após dia nos mais variados ramos de atividade, porém chaves e fechaduras, desde o século XIX, sofreram poucas mudanças nesse sentido (SCRUTTON, 2013).

A empresa sueca Assa Abloy é responsável por fabricar cerca de 10% das fechaduras usadas no mundo e é considerada a maior fabricante mundial de fechaduras. Na sede da empresa, em Estocolmo, encontra-se em fase de testes modelos de fechaduras digitais que possibilitam o acionamento da fechadura com um simples aceno. Outro modelo possibilita a abertura da fechadura fazendo uso da tecnologia *Bluetooth* através de aproximação. As fechaduras digitais, além de seguras, fornecem praticidade para o usuário, pois podem ser incorporadas aos *SIM cards* de aparelhos celulares, *softwares* e até mesmo ao *hardware* do *smartphone*. A incorporação, da fechadura digital no próprio *hardware* do dispositivo, é possível com o uso da tecnologia NFC (SCRUTTON, 2013).

Segundo o presidente executivo da empresa Assa Abloy, Johan Molin:

> Creio que a maioria das pessoas preferirá o sistema digital. As pessoas confiarão mais em uma identidade protegida, distribuída pela internet via celular, do que em uma chave física.

Scrutton (2013) menciona que atualmente nos hotéis as fechaduras eletromecânicas, como cartões, correspondem por

praticamente 50% das vendas da Assa Abloy e o investimento em soluções tecnológicas nessa área é cada vez maior, com um aumento de 129% desde 2005 e 210 milhões de dólares somente no ano de 2012, que corresponde a 2,9% do faturamento total da empresa em pesquisa e desenvolvimento.

A fabricante de fechaduras Schlage, é um exemplo de empresa que investe no desenvolvimento tecnológico nessa área, comercializa uma solução que destrava as portas a quilômetros de distância, a partir de telefones celulares (RICHTEL & KOPYTOFF, 2011).

Soluções de acionamento de fechaduras com smartphone também estão presentes em alguns modelos de carros da Marcedez. O ZipCar, como é chamada a solução, possibilita destrancar a porta do carro ao pressionar um botão do aplicativo (RICHTEL & KOPYTOFF, 2011).

De acordo com Rajeev Chand, chefe de pesquisa da Rutberg & Co, as chaves passarão a ser um objeto arcaico e se tornarão obsoletas ao passar dos anos (RICHTEL & KOPYTOFF, 2011).

### 2.1.4 Fechaduras Modernas

Além das fechaduras que são acionadas com cartões RFID, existem outros modelos que dispensam o uso de chaves convencionais, tais como as fechaduras biométricas e senhas. A empresa Portuguesa nControl, localizada na cidade do Porto, comercializa um modelo de fechadura que oferece as duas opções de acionamento. O modelo NC F500 além de realizar o acionamento através da impressão digital, possui um teclado matricial para a inserção de senhas, dispensando a utilização de uma chave mecânica. O fato de não ter que carregar um objeto cuja única função é abrir a porta é um diferencial se comparada com as demais fechaduras, isso porque diminui o volume carregado pelo usuário e evita eventuais esquecimentos. O modelo NC F500, mostrado na Figura 2, pode armazenar até 500 impressões digitais e 100 senhas[1], simultaneamente. (NCONTROL, 2014).

[1] O tamanho da senha pode variar entre 6 e 10 caracteres.

Figura 2 - Fechadura com biometria e senha
Fonte: NCONTROL (2014)

Outra que se destaca pelo diferencial é a fechadura lançada pela empresa americana *Lockitron* que utiliza um aplicativo, Android ou iOS, e a partir deste é realizada a abertura ou trancamento da fechadura de qualquer lugar do mundo, desde que tenha acesso à internet. A Figura 3 mostra esse modelo de fechadura que utiliza não só o aplicativo para fazer o acionamento da fechadura, mas também por proximidade, utilizando as tecnologias *Bluetooth* e NFC. Para os usuários que não possuem aparelhos celulares com uma dessas tecnologias, é possível abrir ou fechar a porta com o envio de mensagens de texto (LOCKITRON, 2012).

Figura 3 - Fechadura *Lockitron*
Fonte: LOCKITRON (2012)

O mais recente lançamento de fechaduras *high-tech* aconteceu em janeiro deste ano, na cidade de Las Vegas, durante a *Consumer Electronics Show* (CES) 2014. Dotadas de conexão *Bluetooth* 4.0 e NFC, as fechaduras Okidokeys (Figura 4) permite abrir e/ou fechar uma porta através de aplicativos de smartphone, disponibilizado gratuitamente pela empresa, compatíveis com os sistemas operacionais Android e iOS (SOUZA, 2014).

Figura 4 - Fechadura Okidokeys
Fonte: OKIDOKEYS (2014)

A Tabela 1 mostra as principais características e uma breve comparação entre esses três modelos de fechaduras.

Tabela 1 - Comparativo entre fechaduras

| | NC F500 | Lockitron | Okidokey |
|---|---|---|---|
| Tamanho (cm) | 8,5 x 7,2 x 6,8 | 17 x 10,4 x 4,2 | 16 x 7,5 x 4,2 |
| Peso | ND* | ND* | 28,35 g |
| *Bluetooth* | X | ✓ | ✓ |
| NFC | X | ✓ | ✓ |
| Ethernet | X | ✓ | |
| Compatibilidade Android/iOS | X | ✓ | ✓ |
| Key Card | ✓ | ✓ | ✓ |
| Biometria | ✓ | X | X |

Fontes: NCONTROL (2014), LOCKITRON (2012) e OKIDOKEYS (2014)

* Informação não disponível na folha de dados.

### 2.1.5 Protocolos de Comunicação

O setor de automação residencial e/ou predial faz uso de variados protocolos que possuem atributos semelhantes, porém com peculiaridades que devem ser consideradas na fase de elaboração do projeto. A decisão de qual protocolo utilizar deverá ser tomada após análise dos recursos que essas tecnologias oferecem e das características do ambiente a ser automatizado.

Existem no mercado os mais variados tipos de protocolos para domótica e dentre esses protocolos pode-se citar os mais utilizados: CAN, X-10, Modbus, KNX, Z-wave, Insteon, XAP, *Bluetooth* e ZigBee (AURESIDE, 2014). Essas duas últimas tecnologias serviram como base de estudo para a definição da tecnologia a ser utilizada para a comunicação entre os módulos de acionamento e controle, uma vez que a arquitetura da solução geral já estava definida pela equipe de projeto do ISEP.

#### 2.1.5.1 *Bluetooth versus* ZigBee

*A tecnologia Bluetooth* é considerada um padrão sem fio global e devido a sua flexibilidade é utilizada em diversos dispositivos tais como *smartphones*, fones de ouvido, impressoras, *notebooks* entre outros aparelhos (*BLUETOOTH*, 2014).

Essa tecnologia é especificada para a troca de informações em curta distância sem a utilização de fios, com alto rendimento e baixo consumo. Inicialmente a tecnologia foi projetada para ser utilizada em redes com dispositivos e periféricos que compunha uma rede relativamente simples, mas com o passar dos anos as redes *Bluetooth* foram ganhando maiores proporções o que sugere um estudo detalhado da tecnologia antes de ser escolhida e aplicada. Atualmente esse protocolo é utilizado nas mais variadas áreas e em todas elas, o consórcio composto por empresas como 3Com, Compaq, Dell, HP, Motorola, Philips, Samsung e Texas, preocupa-se com inúmeros fatores inclusive os de segurança e interoperabilidade com os demais padrões de tecnologia sem fios existentes no mercado (KOBAYASHI, 2004).

O *Bluetooth* é classificado em classes e são essas classes que determinam a potência de operação e o alcance aproximado. A Tabela 2 mostra as faixas de valores que os dispositivos *Bluetooth* podem assumir considerando cada classe (*BLUETOOTH*, 2014).

Tabela 2 - Classes *Bluetooth*

| Classe | Potencia máxima (mW) | Potencia mínima (mW) | Alcance (m) |
|---|---|---|---|
| Classe 3 | 1 | - | ~1 |
| Classe 2 | 2,5 | 0,25 | até 10 |
| Classe 1 | 100 | 1 | até 100 |

A primeira versão lançada oficialmente foi a 1.2 que possuía uma taxa de transmissão de 1 Mbit/s e a evolução dessa tecnologia é perceptível assim que comparada com as versões lançadas posteriormente, como é o caso da 2.0 e 3.0 que possuem uma taxa de transmissão de 3 Mbit/s e 24 Mbit/s, respectivamente. A versão subsequente foi a 4.0, também chamada de *Bluetooth* LE (*Low Energy*), *Bluetooth Smart* ou simplesmente BLE, que possui a mesma taxa de transmissão da versão anterior, porém com um menor consumo de energia (*BLUETOOTH*, 2014). Segundo Rothman (2010) a versão 4.0 do *Bluetooth* consome 17 vezes menos energia que a versão anterior.

O consórcio responsável pela tecnologia ainda lançou a versão 4.1 que possui as mesmas características da versão anterior, porém com um aperfeiçoamento da funcionalidade de baixo consumo (*BLUETOOTH*, 2014).

Assim como o *Bluetooth*, o ZigBee é um padrão internacional de comunicação sem fio e também conta com uma gama de aplicações nas mais variadas áreas. Até o ano de 2012 mais de 600 produtos, no âmbito residencial e 400 no empresarial, foram certificados com a tecnologia e estima-se que em 2016 haverá aproximadamente 4,3 bilhões de equipamentos que contenham a tecnologia ZigBee instalados em residências e empresas (ZIGBEE, 2014). A Tabela 3 mostra uma breve comparação entra as tecnologias.

Tabela 3 - Comparativo entre *Bluetooth* e Zigbee

| | *Bluetooth* 4.0 | ZigBee | | |
|---|---|---|---|---|
| Padrão | IEEE 802.15.6 | IEEE 802.15.4 | | |
| | | Global | Américas | Europa |
| Frequência de operação | 2.1 a 2.5 GHz | 2.4 GHz | 915 MHz | 868 MHz |
| Taxa de transferência | 270 Kbs | 250 Kbs | 40 Kbs | 20 Kbs |
| Canais | 40 | 16 | 10 | 1 |
| Alcance[3] | ~ 150 metros | 10 a 1600 metros | | |
| Potência | ~ 10 mW | 30 mW | | |
| Topologia | Estrela | Malha | | |
| Rede | PAN | LAN | | |
| Conexão | Síncrona | Assíncrona | | |

Fonte: *BLUETOOTH* (2014) e ZIGBEE (2014).

Apesar do *Bluetooh* e *Zigbee* serem um padrão internacional de comunicação sem fio, é preciso considerar algumas características antes de definir qual das tecnologias será aplicada no projeto (TEXAS INSTRUMENTS, 2010).

O *Bluetooth* foi concebido como uma rede de área pessoal (do inglês *Personal Area Network*, PAN) que são redes sem fio que interligam dispositivos em uma área reduzida. Já o ZigBee foi idealizado como uma rede local (do inglês Local Area Network, LAN), que são mais comuns e assim como a PAN permite interligar computadores, servidores e outros dispositivos em uma área limitada, porém abrange uma área maior que as PAN's (TEXAS INSTRUMENTS, 2010).

Desde o início, o *Bluetooth* foi projetado para operar em uma rede de topologia em estrela, utilizando um nodo central que gerencia a comunicação entre os demais dispositivos. O ZigBee foi projetado para ser utilizado em redes que operam com a topologia em malha, ou seja, os elementos da rede comunicam-se entre si sem a necessidade de um nodo principal de gerenciamento (TEXAS INSTRUMENTS, 2010). A Figura 5

[3] As distâncias de transmissão podem variar de acordo com a potência, condições ambientais, obstáculos e topologia geográfica do ambiente de aplicação.

mostra um comparativo entre as topologias em estrela (esq.) e malha (dir.).

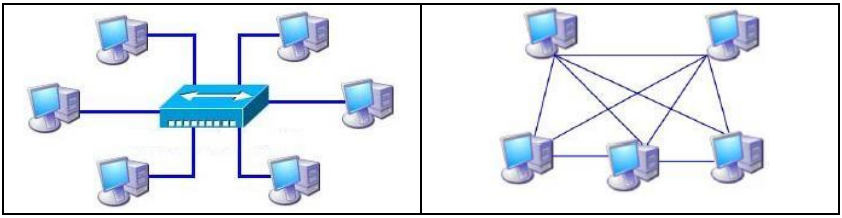

Figura 5 - Comparativo entre as topologias em estrela e malha
Fonte: PEF (2014)

Quando se pergunta qual tecnologia consome menos energia, a resposta depende do cenário de aplicação, pois o BLE utiliza conexão síncrona, isso significa que tanto o mestre quanto o escravo da rede “acordam” juntos e tal característica colabora para o baixo consumo de energia, porém, é necessário aguardar 3 milissegundos para que a conexão seja estabelecida. Por sua vez, o ZigBee opera de forma assíncrona, ou seja, os elementos roteadores da rede ficam constantemente “acordados” e o consumo destes elementos é relativamente alto, porém não há um atraso na hora de estabelecer comunicação com um *end-node* (TEXAS INSTRUMENTS, 2010).

Segundo Decuir (2010), outros fatores devem ser considerados na comparação entre as tecnologias:

- Não há no mercado, PC’s ou *smartphones* com ZigBee, ao contrário do *Bluetooth* que, além dessas áreas, também está consolidado na área automotiva;
- ZigBee é de baixa potência, porém o BLE consome menos energia e
- O *low energy* do *Bluetooth* melhorou o desempenho da tecnologia.

#### 2.1.5.2 NFC

Nesta seção será apresentado o histórico da tecnologia que servirá de base para realizar o acesso ao quarto de hotel, assim como o princípio de funcionamento, áreas de aplicação e

questões relacionadas a segurança na troca de informações utilizando o NFC.

**O que é NFC?**

O NFC é uma tecnologia oriunda do RFID, que permite a comunicação entre dois dispositivos através de radio frequência num cenário em que um dispositivo possui uma fonte de energia e age ativamente sobre outro dispositivo que não necessariamente precisa de uma fonte de alimentação (HECKE, 2011).

Há outras características que descrevem bem a tecnologia NFC, tais como:

- Intuitivo – Todas as operações utilizando o NFC são realizadas com um simples toque;
- Seguro – As trocas de informações são realizadas em curtas distâncias o que acarreta em maior segurança;
- Interoperabilidade – Por pertencer a um fórum e seguirem normas previamente estabelecidas, os mais variados dispositivos que possuem NFC funcionam entre si, independentes do fabricante;
- Aberta e baseada em padrões – As camadas de implementação do NFC seguem normas internacionais como ISO, ECMA, e ETSI.

A NFC aproveitou a popularização dos *smartphones* e ganhou espaço no mercado atuando junto com esses dispositivos. Segundo ABI Research o número de *smartphones* comercializados com a tecnologia NFC integrada teve um aumento de 129% no ano de 2013. Diante desse crescimento destaca-se o segmento *mobile* que representa 4 em cada 5 dispositivos com NFC, e nos próximos anos outros produtos, como câmeras digitais, automóveis e sistemas de som, devem aderir a tecnologia (ACEPI, 2013).

Atualmente são comercializados inúmeros *smartphones* com tal tecnologia podendo-se destacar os modelos LG Nexus 5, que foi utilizado neste projeto, BlackBerry Bold 9900 e 9930,

BlackBerry Curve 9350, 9360 e 9370, Nokia C7 (BRITO, 2012), além do recém lançado iPhone 6.

**Surgimento do NFC**

O NFC é uma tecnologia baseada no RFID que utiliza a identificação por radio frequência para a troca de informações entre dois dispositivos, porém, como visto anteriormente, o alcance do NFC é relativamente baixo se comparado às demais tecnologias sem fio (NFC, 2014).

Foi criado no ano de 2004 um fórum NFC que consiste em um grupo dedicado a criar normas de segurança, facilidades de uso e disseminação da tecnologia. Essa ação foi tomada para garantir a interoperabilidade entre os mais variados dispositivos que possuam a tecnologia NFC, assim todos os fabricantes que desejam incorporar o NFC em seus produtos, devem atender as normas definidas por esse fórum que é composto por empresas de *hardware*, *software*, cartões de crédito e bancos como Qualcomm, LG, Huawei, HTC, Motorola, NEC, RIM, Samsung, Sony, Toshiba, AT&T, Sprint, Google, Microsoft, PayPal, Visa, Mastercard, American Express, Intel e Nokia (BRITO, 2012). Essa última detém o posto de primeira empresa a lançar no mercado um dispositivo compatível com NFC, em 2006 com o modelo 6131 (NFC, 2014).

Atualmente a tecnologia NFC está mais presente na Europa, Ásia e Japão, entretanto os Estados Unidos vem apresentando um crescimento significativo nos últimos anos e estima-se que em breve o NFC será uma tecnologia popular em se tratar de troca de informações em curtas distâncias (NFC, 2014).

**No que o NFC pode ser utilizado?**

A NFC possui uma gama de aplicações, uma série de facilidades para os usuários e foi idealizada para a transmissão segura de dados. Enquanto o RFID é a tecnologia mais apropriada para aplicações nas quais os dois dispositivos, que precisam se comunicar, não estão necessariamente próximos um do outro, a NFC realiza a troca de informações em situações em

que os dispositivos encontram-se a alguns centímetros de distância. Essa característica oferece maior segurança aos usuários, pois inibe a intercepção de dados por pessoas má intencionadas ou sem autorização para visualizar os dados (HECKE, 2011).

A operadora Vodafone lançou um serviço, que utiliza a NFC, que fornece permissão aos clientes de armazenar centenas de cartões promocionais, de trânsito ou fidelidade. Essa funcionalidade visa extinguir esses cartões, que antes ocupavam os espaços nas carteiras e gavetas, e concentrá-los nos *smartphones*, liberando espaços físicos e evitando esquecimentos. Atualmente esse sistema possui mais de um milhão de usuários em países como Alemanha, Holanda e Espanha e a tendência é que até o final de 2014 outros países, em que a empresa opera, adiram ao serviço. Com esse serviço o cliente poderá carregar o atual cartão de plástico dentro de seu *smartphone* bastando fotografar ambos os lados do cartão com a própria câmera do *smartphone* ou digitar o número do cartão no aplicativo (CLARK, 2014).

Existem outras aplicações que exemplificam a facilidade que o NFC pode proporcionar aos usuários como, por exemplo, no Japão é possível comprar bilhetes de metrô e trem, ingressos de eventos e até realizar operações bancárias e pagamentos em estabelecimentos comerciais através de *smartphones* com NFC. A divulgação de filmes é outro exemplo de aplicações que usam o NFC, no qual é possível carregar nos cartazes de divulgação um código que possibilita o usuário assistir ao trailer do filme em questão (BRITO, 2012).

**Como o NFC funciona?**

A NFC possui certa semelhança com o *Bluetooth* e o Wifi considerando que as três tecnologias são utilizadas para a troca de informações entre dispositivos, como *smartphones*, sem a utilização de fios. Uma das diferenças entre essas tecnologias é a forma em que os dados são transmitidos, enquanto o *Bluetooth* e o Wifi utilizam sinais de rádio, a NFC faz uso de campos magnéticos (NFC, 2014).

Como mencionado anteriormente, o NFC é uma tecnologia oriunda do RFID, que utiliza a identificação por radio frequência,

porém a NFC possui uma particularidade, na qual ambos os dispositivos envolvidos da transmissão de dados, precisam estar relativamente próximos um do outros, essa distância deve ser de no máximo 10 centímetros (NFC, 2014).

A tecnologia NFC faz uso da indução magnética para realizar a comunicação, na qual o leitor emite uma baixa corrente elétrica que gera um campo magnético que atravessa o espaço físico entre os dispositivos. Essa pequena corrente elétrica, emitida pelo leitor chega até o dispositivo a ser lido por uma bobina e é transformada novamente em impulso elétrico para responder algum dado que pode ser um número de identificação ou qualquer outra informação (NFC, 2014).

**Tipos de Tag**

Antes de mencionar os diferentes modos de operação da NFC, é necessário entender o conceito de *tag*. Também chamadas de etiquetas NFC, as *tags* são componentes simples compostos por uma antena e uma unidade de memória com baixa capacidade de armazenamento (UBITAP, 2014). A estrutura de uma tag NFC está ilustrada na Figura 6.

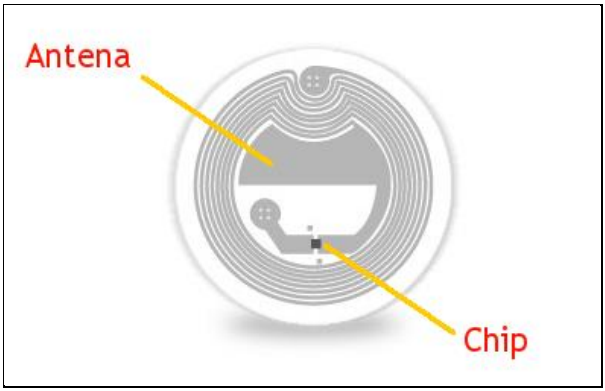


Figura 6 - Tag NFC
Fonte: UBITAP (2014)

Dispositivos que utilizam NFC podem operar de duas formas: passivamente ou ativamente. No caso de um passivo, como por exemplo, as *tags* NFC, um dispositivo gera o campo de radiofrequência e o outro, nesse caso a *tag*, utiliza esse campo para se enviar as informações. Os dispositivos passivos contêm informações que outros dispositivos podem ler, em contrapartida não conseguem ler informações providas de outras tags. É possível compreender melhor o conceito de dispositivos passivos fazendo uma analogia com um cartaz fixado na parede, o qual é capaz de repassar informações, mas o cartaz em si, não recebe qualquer informação. Já os dispositivos ativos, como os *smartphones*, geram seus próprios campos eletromagnéticos usando a fonte de energia interna e são capazes de não somente ler informações das *tags* NFC, mas também de trocarem informações com outros dispositivos compatíveis, podendo, inclusive, alterar as informações das *tags*, caso tenham permissão para tal ação (NFC, 2014).

# 3 DESENVOLVIMENTO

Neste capítulo será descrito o desenvolvimento do projeto, que visa cumprir os objetivos descritos na Seção 1.2.

Serão abordados os resultados do estudo realizado (levantamento de requisitos) na forma de variáveis envolvidas no processo de automação, as características do cenário no qual poderá ser aplicada a solução e o principio de funcionamento.

O protótipo do módulo de acionamento da fechadura (MAF) foi concebido em uma placa do Arduino Duemilanove (Figura 7), que contém o microcontrolador ATMEGA328P e as interfaces necessárias para o desenvolvimento do módulo de acionamento da fechadura. Para o desenvolvimento do *firmware* foi utilizada a IDE (Integrated Development Environment) do próprio Arduíno.

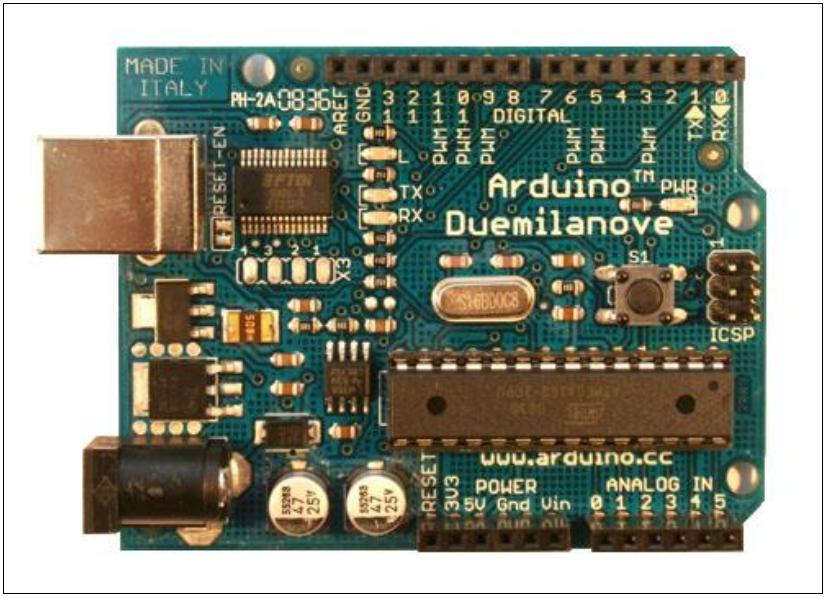


Figura 7 – Arduino Duemilanove
Fonte: Arduino (2009).

Foi utilizado para fins de validação de conceito, além do Arduino, o módulo NFC V2.0 fornecido pela empresa Elechouse, a fechadura NFC fabricada pela empresa Confitek, além do

módulo *bluetooth*. Estes quatro componentes serão abordados com mais detalhes na Seção 3.3.

## 3.1 VISÃO GERAL

A Figura 8 ilustra uma visão geral da solução, além dos protocolos de comunicação utilizados para conectar os diferentes módulos. A solução geral é composta por sensores e módulos atuadores comandados por um controlador central, que aciona os recursos de um quarto de hotel como fechadura, televisão, ar condicionado, lâmpadas e persianas. Além disso, é possível realizar esse controle através de um aplicativo, compatível com o sistema operacional Android, no qual interage com servidores de serviços internos e externos através de uma rede local. Toda essa estrutura opera sob a supervisão de um software instalado no computador localizado na recepção do hotel.

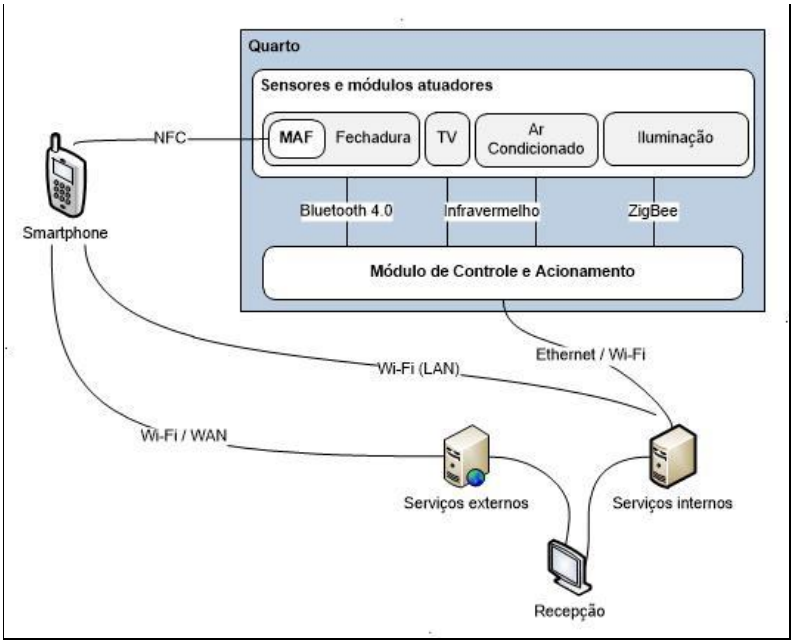


Figura 8 - Visão geral da solução

O foco principal deste projeto é o desenvolvimento do módulo de acionamento da fechadura (MAF) do quarto do hotel utilizando a tecnologia NFC. É importante mencionar que o módulo de controle e acionamento (MCA), é um elemento fundamental para o perfeito funcionamento da solução proposta neste trabalho e para todos os efeitos considera-se esse módulo uma caixa preta já desenvolvida. A Figura 9 Figura 9 – apresenta uma visão sucinta da solução proposta neste projeto.

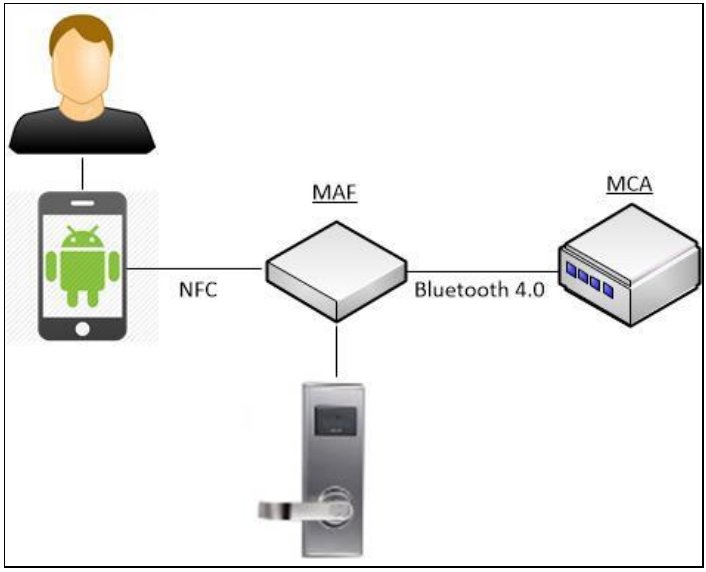


Figura 9 – Cenário de aplicação

A solução proposta por este trabalho consiste na utilização de *smartphones* para acionar a abertura da fechadura do quarto de hotel, ou seja, ao realizar o *check-in* na recepção do hotel, o código NFC atrelado ao *smartphone* do hóspede recebe permissão de acesso a um determinado quarto. Quando o usuário aproxima o *smartphone* da fechadura, o módulo de acionamento consulta o controlador do quarto que, por sua vez, consulta a permissão de acesso no banco de dados que caso seja permitida o módulo de acionamento abre a fechadura, caso contrário esta permanecerá na posição padrão, ou seja, fechada.

Considerando o cenário de aplicação e as características previstas para o MAF, foi definida a utilização do *bluetooth*, ao

invés do *zigbee*. Tal decisão foi tomada após o estudo de ambas as tecnologias, na qual o *bluetooth* apresenta vantagens nos seguintes fatores:

- Topologia da solução em estrela;
- Taxa de transmissão;
- Alcance e, principalmente
- Baixo consumo de energia;

## 3.2 COLETA E ANÁLISE DE REQUISITOS

Esta seção tem por objetivo apresentar os principais documentos, diagramas e tabelas que foram desenvolvidos durante as fases de concepção e elaboração do projeto.

### 3.2.1 Levantamento de Requisitos

A Tabela Tabela 4 - Requisitos Funcionais4 apresenta a lista de requisitos funcionais e a Tabela 5 mostra os requisitos não funcionais a serem atendidos pela solução proposta. Estes requisitos foram definidos baseados nos resultados obtidos através do estudo realizado de soluções semelhantes e reuniões com o time de projeto, visando melhorar algumas e agregando outras funcionalidades.

Tabela 4 - Requisitos Funcionais

| ID | Descrição |
|---|---|
| 01 | O MAF deverá obter os dados de identificação de um smartphone. |
| 02 | O MAF deverá enviar o ID do NFC do smartphone para o controlador. |
| 03 | O MAF deverá receber a resposta do controlador principal e transformá-la em informação útil ao usuário. |
| 04 | O MAF deverá informar de forma visual, se usuário possui ou não a permissão de acesso solicitada. |
| 05 | O MAF deverá informar de forma sonora, se usuário possui ou não a permissão de acesso solicitada. |
| 06 | O MAF deverá ter alimentação elétrica interna. |

Tabela 5 - Requisitos não Funcionais

| ID | Descrição |
|---|---|
| 01 | O desempenho do módulo deve ser considerado por corresponder a um fator de qualidade. |
| 02 | O consumo de energia do módulo deve ser considerado por corresponder a um fator de qualidade. |

### 3.2.2 Regras de Negócio

Regras de negócio são políticas, condições ou restrições que devem ser consideradas na execução dos processos existentes em uma organização. A Tabela 6 apresenta as regras de negócio adotadas para o desenvolvimento deste projeto.

Tabela 6 - Regras de Negócio

| **RN01** | |
|---|---|
| Objetivo | Comunicação entre o módulo de acionamento e o controlador |
| Descrição | A comunicação será através da tecnologia *Bluetooth* versão 4.0. |
| Histórico | Data de identificação: 11/03/2014 |
| **RN02** | |
| Objetivo | Comunicação entre o módulo de acionamento e o smartphone |
| Descrição | A comunicação será através da tecnologia NFC. |
| Histórico | Data de identificação: 11/03/2014 |
| **RN03** | |
| Objetivo | Energização do módulo |
| Descrição | O módulo de acionamento será alimentado através de quatro pilhas elétricas AA. |
| Histórico | Data de identificação: 17/03/2014 |
| **RN04** | |
| Objetivo | Posição padrão da fechadura |
| Descrição | Considera-se a posição padrão da fechadura como fechada. |
| Histórico | Data de identificação: 11/03/2014 |

| **RN05** | |
|---|---|
| Objetivo | *Feedback* de acesso permitido |
| Descrição | Ao receber a resposta de acesso permitido do controlador, o MAF deverá abrir a fechadura. |
| Histórico | Data de identificação: 17/03/2014 |
| **RN06** | |
| Objetivo | *Feedback* de acesso permitido |
| Descrição | Ao receber a resposta de acesso permitido do controlador, o MAF deverá acender um LED de cor verde e com duração de 200 milissegundos. |
| Histórico | Data de identificação: 17/03/2014 |
| **RN07** | |
| Objetivo | *Feedback* de acesso permitido |
| Descrição | Ao receber a resposta de acesso permitido do controlador, o MAF deverá emitir um bipe sonoro com duração de 200 milissegundos. |
| Histórico | Data de identificação: 17/03/2014 |
| **RN08** | |
| Objetivo | *Feedback* de acesso negado |
| Descrição | Ao receber do controlador a resposta de acesso negado, o MAF deverá manter a fechadura na posição padrão. |
| Histórico | Data de identificação: 17/03/2014 |
| **RN09** | |
| Objetivo | *Feedback* de acesso negado |
| Descrição | Ao receber do controlador a resposta de acesso negado, o MAF deverá acender um LED de cor vermelha durante 1 (um) segundo. |
| Histórico | Data de identificação: 17/03/2014 |
| **RN10** | |
| Objetivo | *Feedback* de acesso negado |
| Descrição | Ao receber a resposta de acesso negado do controlador, o MAF deverá emitir um bipe sonoro com 1 (um) segundo de duração. |
| Histórico | Data de identificação: 17/03/2014 |

| RN11 | |
|---|---|
| Objetivo | *Stand By* |
| Descrição | Enquanto não estiver sendo utilizado, o MAF deverá mostrar continuamente um LED aceso na cor azul. |
| Histórico | Data de identificação: 17/03/2014 |

### 3.2.3 Diagrama de Sequência

A Figura 10 mostra o diagrama de sequência para uma situação de sucesso, ou seja, o usuário aproxima o *smartphone* com NFC do módulo de acionamento, este último lê as informações do *smartphone* e solicita acesso ao controlador do quarto. O controlador consulta a base de dados e verifica que a solicitação de acesso é permitida e essa resposta é enviada para o módulo de acionamento que por fim realiza a abertura da fechadura.

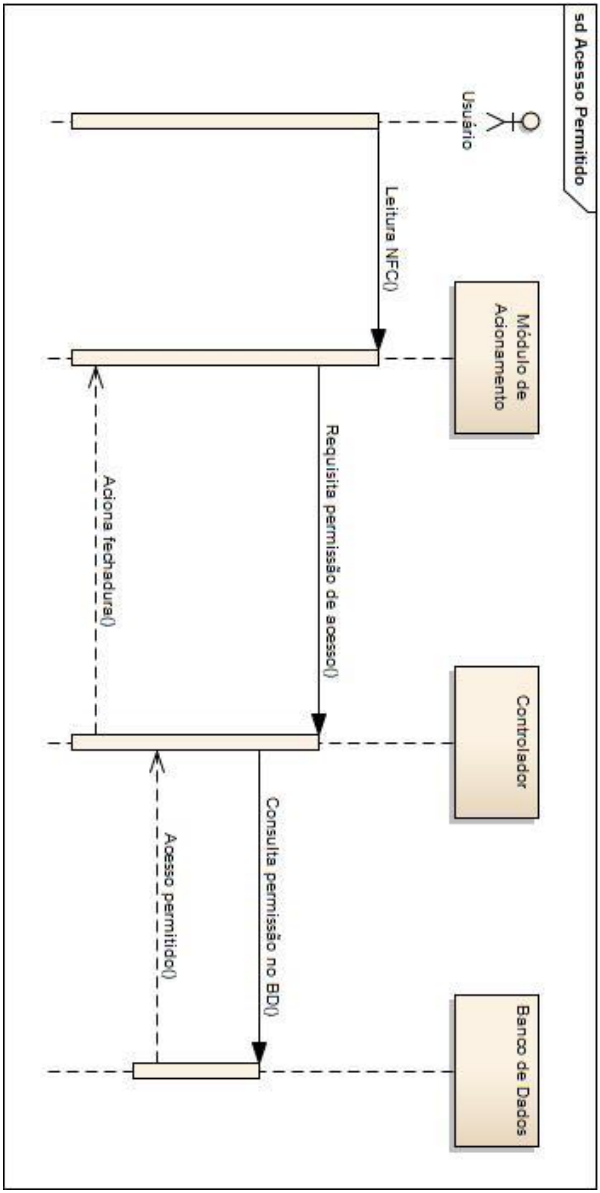


Figura 10 - Diagrama de sequência para acesso permitido

O diagrama de sequência representado pela Figura 11mostra uma situação de acesso negado, ou seja, como mostrado na situação anterior, o usuário aproxima o *smartphone* com NFC do módulo de acionamento que lê as informações e solicita o acesso ao controlador do quarto. Esse último consulta a base de dados e verifica que o acesso solicitado não é permitido. O controlador envia para o módulo de acionamento a informação de acesso negado que mantém a fechadura na posição padrão, fechada.

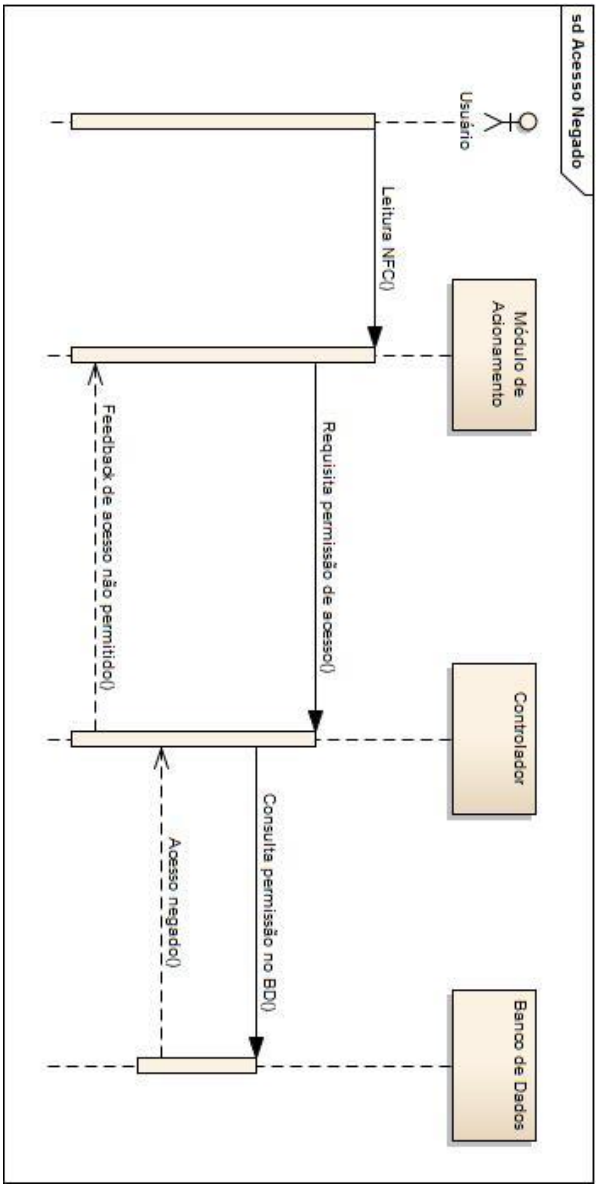


Figura 11 - Diagrama de sequência para acesso negado

## 3.3 ARQUITETURA DO MAF

A Figura 12 **Erro! Fonte de referência não ncontrada.**ilustra a arquitetura de *hardware* do MAF, cuja função é representar os módulos internos necessários para que o módulo embarcado seja empregado na solução geral mostrada na Figura 8, de modo que atenda aos requisitos de conectividade do sistema. Todos os elementos de *hardware* são controlados por um microcontrolador (MCU) central, exceto a fonte de alimentação interna e o bloco regulador de tensão.

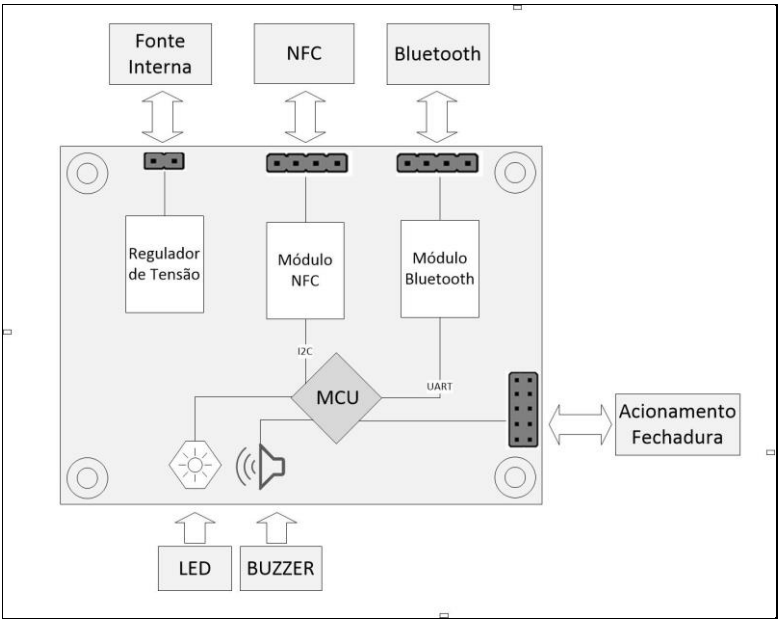


Figura 12 - Arquitetura MAF

Vale lembrar que a utilização dos módulos PN532 (NFC) e HC-05 (Bluetooth) é temporária e está incluída na arquitetura do MAF apenas para validação de conceito. O objetivo dessa representação da arquitetura do MAF é mostrar como o protótipo foi concebido e que futuramente esses módulos serão incorporados à solução, de forma que o NFC, o *Bluetooth* e o microcontrolador estejam inseridos em uma só placa.

Essa Seção descreve os blocos que compõe o protótipo a ser construído. Em alguns casos, como o circuito de *clock* e o regulador de tensão já estão embutidos na placa do Arduino, porém foram desenvolvidos pensando na montagem do protótipo exclusivo do MAF.

### 3.3.1 Esquema Elétrico

Para a construção do esquema elétrico do módulo de acionamento da fechadura foi utilizado o *software* Protheus versão 8. O circuito regulador de tensão e de *clock*, que estão embutidos no Arduino, foram reproduzidos. Já os conectores para a conexão dos módulos *bluetooth* e NFC, acionamento dos LEDs, buzzer e relé, foram incorporados ao esquema elétrico. A Figura 13 apresenta como ficou organizada a arquitetura do MAF.

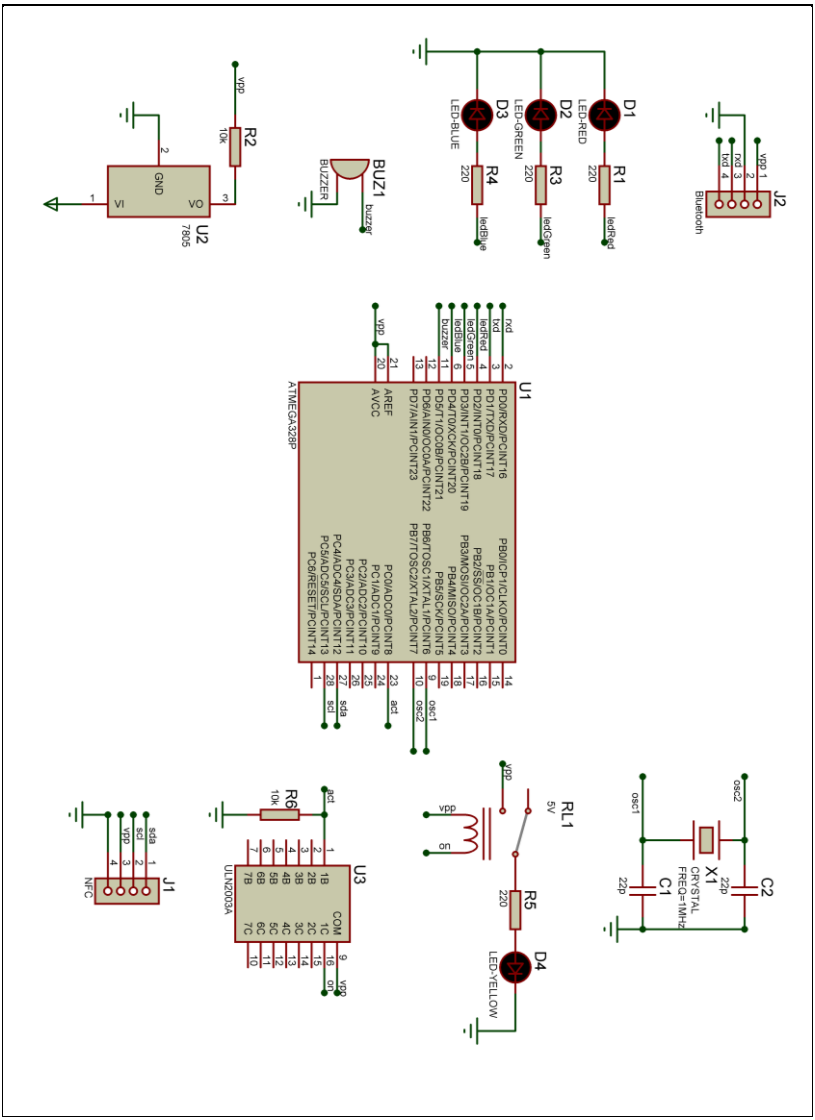


Figura 13 - Esquema elétrico do MAF

### 3.3.2 Layout do Protótipo

A placa do MAF não foi confeccionada pelo fato de o protótipo utilizar módulos externos, nos quais o produto deverá incorporar no layout final. A Figura 14 apresenta o layout do protótipo do MAF.

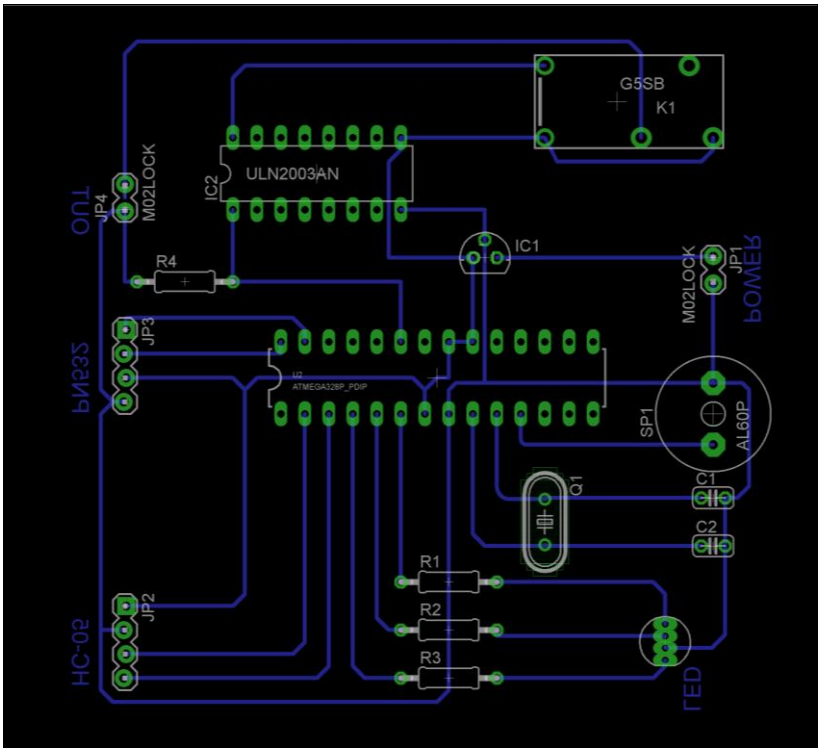


Figura 14 - Layout da placa protótipo do MAF

### 3.3.3 Fonte Interna

Este bloco tem como função fornecer tensão elétrica para alimentar os blocos que compõe o módulo, assim como o microcontrolador e os demais componentes da placa. A energia, conforme preestabelecido, é interna e provida de quatro pilhas AA. A Figura 15 representa o suporte das pilhas que futuramente será utilizado na montagem do protótipo especifico do MAF.

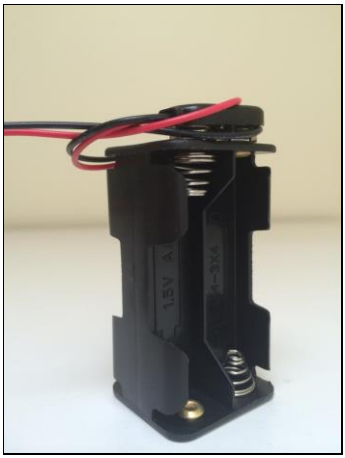

Figura 15 - Suporte das pilhas AA

### 3.3.4 Regulador de Tensão

Regular a tensão fornecida pela fonte interna para o nível de tensão de operação dos módulos e dos elementos que compõe o *hardware* do MAF (5V), é a função do bloco regulador de tensão que tem como principal componente o circuito integrado 7805.

### 3.3.5 Módulo NFC

Responsável pela leitura do NFC foi escolhido o módulo NXP PN532 (Figura 16) por ser popular na área de NFC além da

empresa fornecer documentação técnica para auxiliar os desenvolvedores em seus projetos.

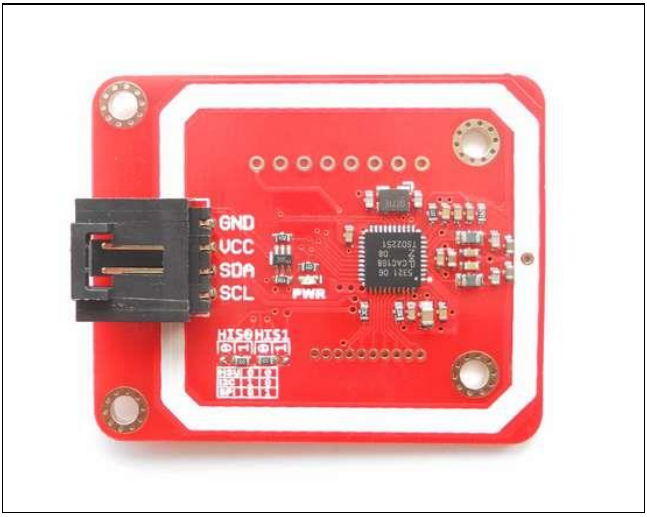


Figura 16 - Módulo PN532 NFC
Fonte: ELECHOUSE (2014)

Seguem abaixo algumas características do módulo:

- Suporte a leitura e escrita nos modos NFC ou RFID;
- *Plug and play*;
- Distância de leitura ente 6 e 4 cm;
- Tensão de operação: 5V TTL para I2C ou UART, 3,3V TTL para SPI e
- Permite a troca de dados com outros dispositivos NFC, como *smartphones*.

O microcontrolador é o responsável por gerar o *clock* utilizado pelo módulo NFC e também por enviar requisições de leitura dos cartões fazendo com que, no cenário em que será utilizado o MAF, os papéis de *master* e *slave* sejam assumidos respectivamente pelo microcontrolador e o módulo NFC. A interface utilizada para comunicação entre o microcontrolador e o módulo NFC foi a I2C, que é configurada através de dois resistores conforme mostrado na Figura 17.


Figura 17 - Configuração UART do módulo NFC
Fonte: ELECHOUSE (2014)

### 3.3.6 Módulo *Bluetooth*

De acordo com o estudo comparativo entre o *bluetooth* e *zigbee* para decidir qual tecnologia é mais apropriada para a solução, foi concluído que, considerando as características do ambiente em que a solução será utilizada, a tecnologia mais indicada é a versão 4.0 do *bluetooth*. Assim como os demais módulos, o *bluetooth* foi disponibilizado pelo ISEP e por não possuir um módulo da versão 4.0, foi utilizado no projeto o módulo HC-05 que opera na versão 3.0. Este módulo é comercializado pela empresa WIDE e foi adaptado em uma PCI por alunos do ISEP para que fosse possível a utilização em matriz de contato.

A Figura 18 mostra o módulo *bluetooth* em questão.

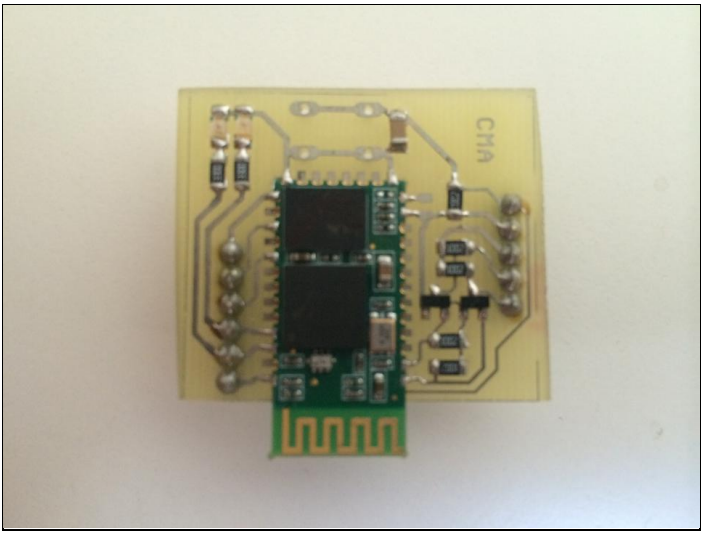

Figura 18 - Módulo *Bluetooth*

Este módulo *bluetooth* pode assumir tanto o papel de *master* quanto *slave* (*default*), este último é o modo utilizado no MAF. O fato de o módulo possuir essa flexibilidade possibilitou a utilização deste no *hardware* do MAF e do MCA.

Seguem abaixo algumas especificações do módulo.

Quadro 1 - Especificações do módulo Bluetooth

| | |
|---|---|
| Tensão de operação | 5V |
| Modos de operação | Master / Slave |
| Comando AT | Sim |
| Dimensões (mm) | 26,9 x 13 x 2,2 |
| Frequência de operação | 2,4 GHz |
| Potencia | ≤ 4 dBm |
| Taxa assíncrono (Max) | 2.1 Mbps |
| Taxa sincrono | 1 Mbps |
| Criptografia | Sim |
| Temperatura | -5 ~ 45º C |

### 3.3.7 Controlador

O primeiro protótipo foi desenvolvido utilizando o Arduino Duemilanove, que contém o microcontrolador ATMEGA328P e

as interfaces necessárias para o desenvolvimento do módulo de acionamento da fechadura. O Quadro 2 mostra algumas das características deste que é o principal componente do MAF.

Quadro 2 - Especificações do Arduino Duemilanove

| | |
|---|---|
| Microcontrolador | ATmega368 |
| Tensão de operação | 5V |
| Tensão de entrada | 7-12V |
| I/O Digital | 14 |
| Entrada analógica | 6 |
| Corrente DC I/O | 40 mA |
| Memória Flash | 32 Kb |
| SRAM | 2 Kb |
| Comparador | 2 |
| EEPROM | 1 Kb |
| Clock | 16 MHz |
| Quantidade de pinos | 28 |
| UART | Pino 0 (RX) / Pino 1 (TX) |
| I2C | A4 (SDA) / A5 (SCK) |
| Interrupções externas | Pinos 2 e 3 |
| PWM | Pinos 3, 5, 6, 9 10 e 11 |

O *firmware* está organizado da seguinte forma: 5 das 14 I/O digitais estão configuradas como saídas, pois são através desses pinos que são acionados os LEDs (PD2, PD3, PD4), o Buzzer (PD5) e o relé (PC0). Das seis entradas analógicas duas (A4-SDA / A5-SCK) são utilizadas para a comunicação I2C, ou seja, entre o microcontrolador e o módulo NFC. Os pinos 0 (RX) e 1 (TX), são responsáveis pela comunicação serial, interface na qual é realizada a comunicação entre o microcontrolador e o módulo *Bluetooth*.

Essa organização foi definida com base nas características do microcontrolador, minimizando assim o trabalho de alteração do *firmware* quando for realizada a migração da solução do Arduino para o protótipo específico.

### 3.3.8 LED de Interação

O MAF possui um padrão de resposta visual que visa informar o usuário sobre a situação do módulo. Foram utilizados três diodos emissores de luz (do inglês LED, *Light Emitting*

*Diode*) que mais tarde, na montagem do protótipo específico do MAF, serão substituídos por um LED RGB. Essa resposta visual tem como objetivo informar os três estados distintos que o módulo pode assumir, conforme mostrado na Tabela 7.

Tabela 7 - Estado do LED de Interação

| Cor / Estado | Azul | Verde | Vermelho |
|---|---|---|---|
| *Stand By* | X | | |
| Sucesso | | X | |
| Falha | | | X |

O primeiro estado é o *Stand By*, que deixa o LED aceso constantemente na cor azul, até que alguma solicitação de acesso seja realizada. O segundo estado liga o LED na cor verde, o qual informa o usuário que o acesso solicitado é permitido. O terceiro e último estado que o MAF pode assumir é o de negação, informa ao usuário que o acesso solicitado não é permitido, através do LED que liga na cor vermelha.

### 3.3.9 Alertas Sonoros

Além de sinais visuais o MAF possui sinais de *feedback* sonoros que buscam informar ao usuário sobre o resultado de cada solicitação de acesso. A Tabela 8 mostra o comportamento dos alertas sonoros de acordo com cada tipo de ação.

Tabela 8 - Estados dos Alertas Sonoros

| Bipes / Estado | Quantidade |
|---|---|
| *Stand By* | 0 |
| Sucesso | 1 |
| Falha | 3 |

Toda solicitação realizada pelo MAF que recebe como resposta uma negação do acesso, será acionado três vezes o bipes que visa informar ao usuário que o acesso ao quarto não é permitido. O MAF emite também um único bipe sempre que o MAF receber a confirmação de permissão de acesso ao quarto. Quando está em *Stand By*, o módulo não emite qualquer tipo de alerta sonoro.

### 3.3.10 Fechadura

A fechadura utilizada no projeto é um modelo disponibilizado pelo ISEP, fabricado pela empresa Confitek e possui de fábrica a interface NFC. A ideia da utilização desta fechadura foi a substituição das placas responsáveis pela leitura NFC e acionamento, originais do produto, pelo MAF. A Figura 19 mostra a fechadura utilizada assim como as placas da solução original que foram substituídas.

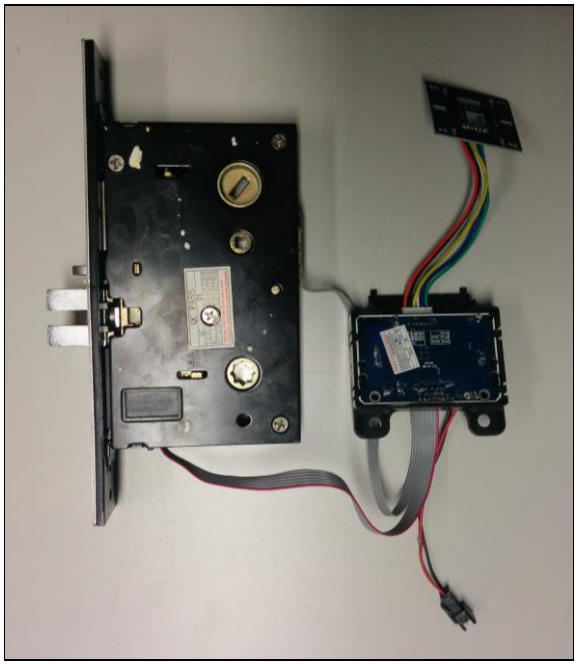

Figura 19 - Fechadura utilizada no projeto

### 3.3.11 Lista de Materiais

A Tabela 9 mostra a lista de componentes, os respectivos preços assim como o valor total necessário para a montagem do protótipo do MAF.

Tabela 9 - Lista de materiais para a montagem do protótipo

| Quantidade | Descrição | Preço unitário |
|---|---|---|
| 01 | Suporte para 4 pilhas | R$ 3,50 |
| 01 | Regulador de tensão 7805 | R$ 1,50 |
| 04 | Pilha AA | R$ 7,00 |
| 01 | Módulo NXP PN532 NFC | R$ 50,50 |
| 01 | Módulo *Bluetooth* | R$ 28,70 |
| 01 | Microcontrolador ATMEGA238P | R$ 18,00 |
| 01 | LED RGB | R$ 4,30 |
| 01 | Buzzer | R$ 1,50 |
| 02 | Conector 1x4 | R$ 0,80 |
| 02 | Conector 1x2 | R$ 0,40 |
| 01 | Relé 5V | R$ 4,50 |
| Total[4] | | R$ 121,10 |

## 3.4 *FIRMWARE* DO MAF

O firmware do MAF possui um laço principal que logo no inicio verifica o funcionamento do módulo NFC e informa se há problemas de conexão. Essa característica foi implementada considerando que a solução deixa de fazer sentido sem esse módulo. Após essa verificação o módulo fica em *stand by* e verificando constantemente se alguma *tag* NFC foi aproximada do módulo. Assim que o módulo faz a leitura da *tag*, o firmware armazena o ID em uma variável e envia para o MCA, para fins de consulta de permissão, e fica aguardando uma resposta. A partir desse ponto o algoritmo pode seguir por três diferentes caminhos: Acesso permitido, acesso negado e *timeout*. Nos dois primeiros o módulo realiza os procedimentos referentes a cada funcionalidade conforme os requisitos e regras de negócios definidos. Por fim, se o módulo ficar esperando a resposta do MAF por mais de três segundos, o módulo retorna para o estaod de *stand by*.

O fluxo principal do firmware do MAF pode ser melhor compreendido através do fluxograma representado na Figura 20.

[4] O valor total não inclui os valores da PCI e mão-de-obra.

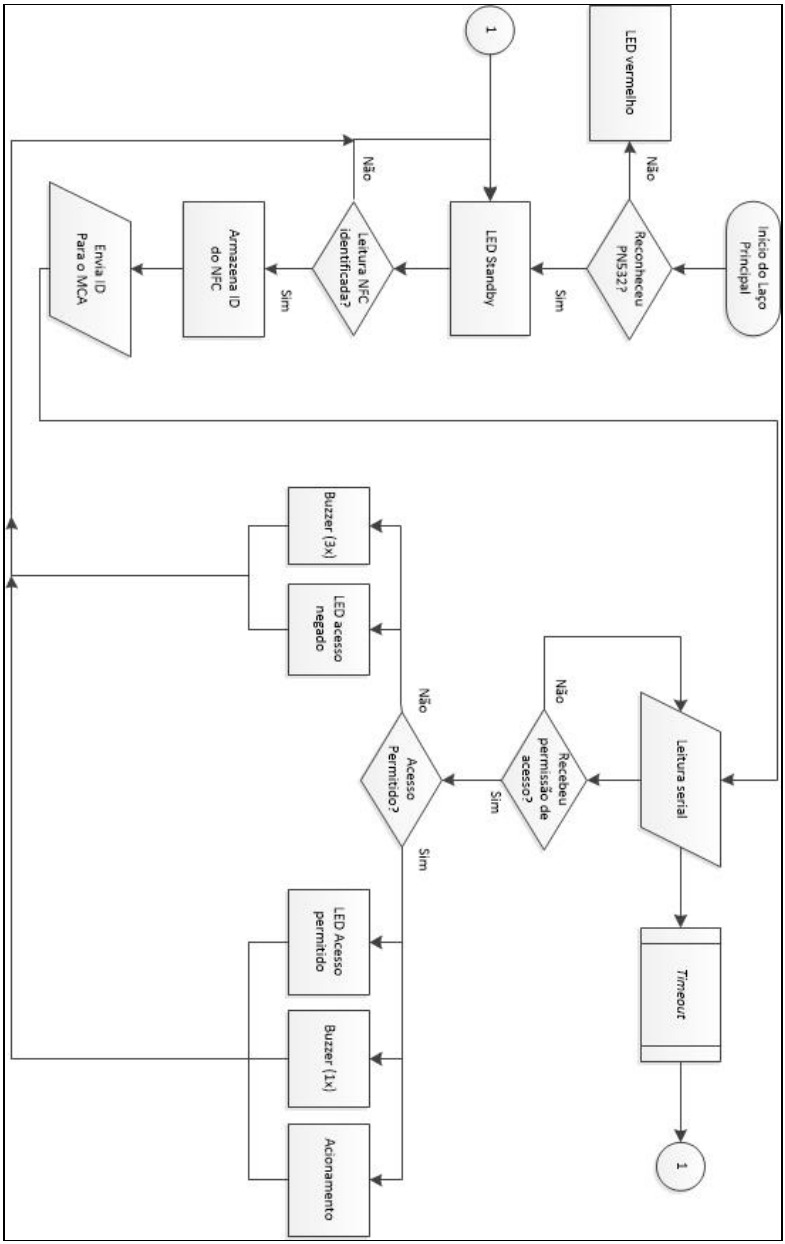


Figura 20 - Fluxograma da solução

# 4 RESULTADOS

Nesse capítulo é apresentado o ambiente de testes, o protótipo do MAF, o qual foi submetido a variados testes unitários e funcionais, assim como os resultados obtidos.

## 4.1 AMBIENTE DE TESTES

O ambiente de testes no qual foi testada a solução, foi o laboratório do GECAD (Grupo de Investigação em Engenharia do Conhecimento e Apoio à Decisão). O local foi escolhido por apresentar características semelhantes ao do quarto de hotel, local em que se propõe a utilização do MAF e MCA, ou seja, um ambiente aberto, com uma área de aproximadamente 40 m² e isento de obstáculos.

A Figura 21 mostra a planta baixa do ambiente de testes, assim como a disposição dos móveis e a localização dos protótipos do MAF e do módulo de controle e acionamento (MCA).

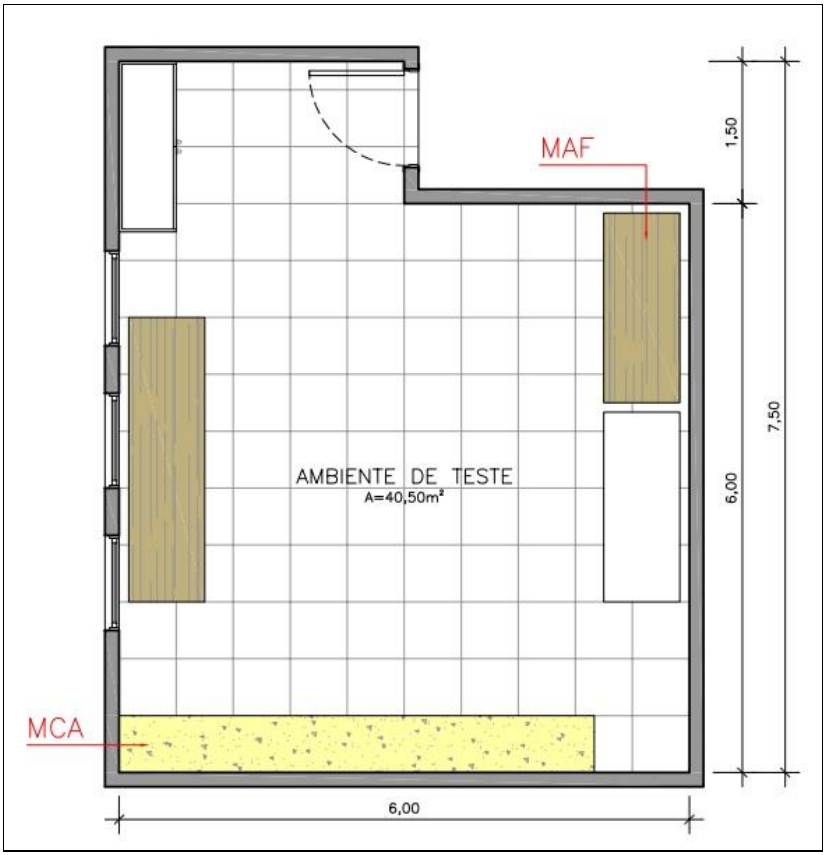


Figura 21 - Planta baixa do ambiente de testes

A Figura 22 mostra como ficou a montagem do primeiro protótipo do MAF que foi utilizado para a realização dos testes unitários e funcionais.

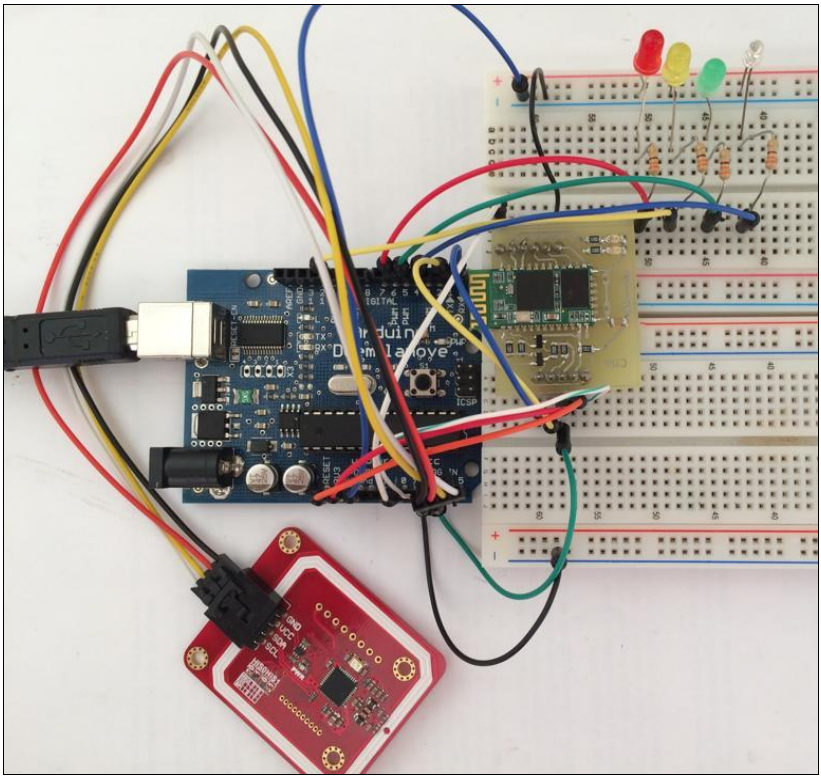

Figura 22 – Protótipo do MAF

## 4.2 TESTES UNITÁRIOS

Esta Seção descreve os testes unitários os quais o protótipo desenvolvido foi submetido além dos resultados esperados e obtidos. Os testes foram idealizados com base no diagrama de sequência descrito na Seção 3.2.3. O *check list* contendo o nome e descrição dos testes realizados pode ser consultado no Apêndice I.

### 4.2.1 Reconhecimento do Módulo NFC

Por diversas vezes, durante os testes do protótipo, o MAF não respondia quando um cartão era aproximado do módulo NFC PN532 devido a mau contato ou falta de conexão, e isso acarretava em tempos de investigação até que o problema fosse solucionado. Sendo assim, foi idealizado um modo para informar aos gestores e desenvolvedor do sistema que o módulo NFC não foi reconhecido pelo MAF, através do LED vermelho aceso constantemente, como mostra a Figura 23.

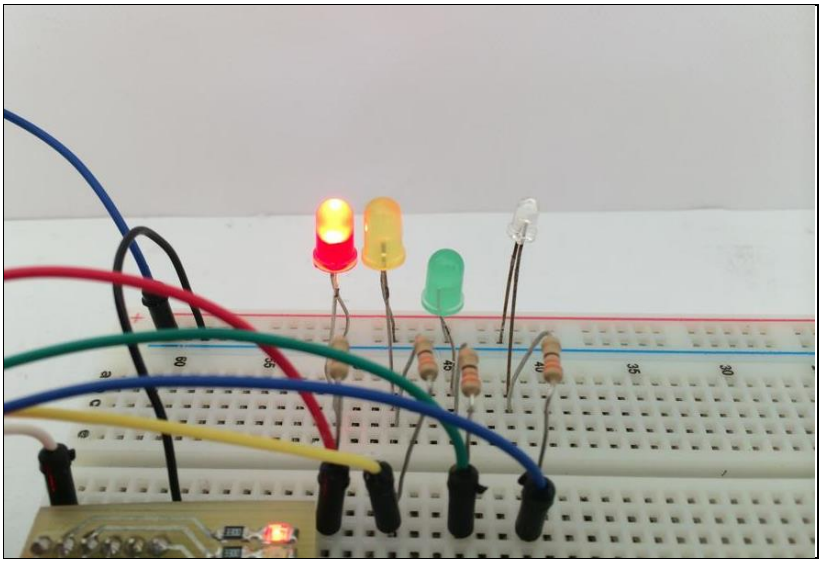

Figura 23 - Feedback de não reconhecimento do módulo NFC

Com esse LED aceso constantemente o MAF não realizou qualquer operação, uma vez que a solução deixa de fazer sentido sem o módulo NFC.

Esse teste consistiu em ligar o MAF com o módulo NFC e operar a solução normalmente. Em seguida o MAF foi desligado, as ligações do PN532 foram desconectadas e o MAF foi religado, apresentando o LED vermelho aceso constantemente, validando assim essa funcionalidade.

### 4.2.2 Leitura do NFC

O primeiro teste realizado foi a leitura do NFC, que consiste em aproximar uma *tag*, simulando um *smartphone*, do módulo PN532 e capturar o código identificador do aparelho.

Para validar essa funcionalidade foi utilizado o aplicativo NFC Tools que, instalado no *smartphone* LG Nexus 5 (Figura 24), faz a leitura do código NFC de uma *tag*.

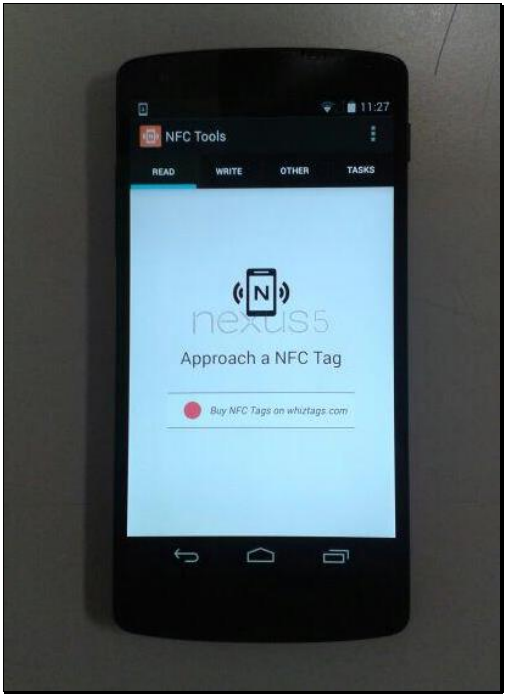


Figura 24- App NFC tools no *smartphone* Nexus 5

Foi usado um cartão NFC genérico e o cartão pessoal de acesso aos laboratórios do ISEP (que também opera com NFC). Ao aproximar os cartões do smartphone, foi possível adquirir o código identificador de cada cartão.

A Tabela 10 mostra o código identificador de cada cartão utilizado durante os testes do MAF.

Tabela 10 - Código ID dos cartões NFC

| Cartão | Código ID |
|---|---|
| Genérico | 2B:55:30:98 |
| ISEP | 8A:B1:B4:D1 |

As Figuras 25 a 28 mostram o cartões e as respectivas telas do aplicativo que informa o ID de cada cartão.

Figura 25 - Tag genérica NFC

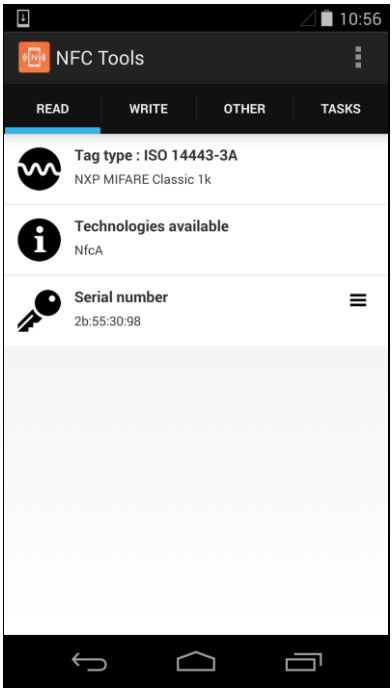


Figura 26 - Código ID NFC do cartão genérico


Figura 27 - Cartão de acesso NFC

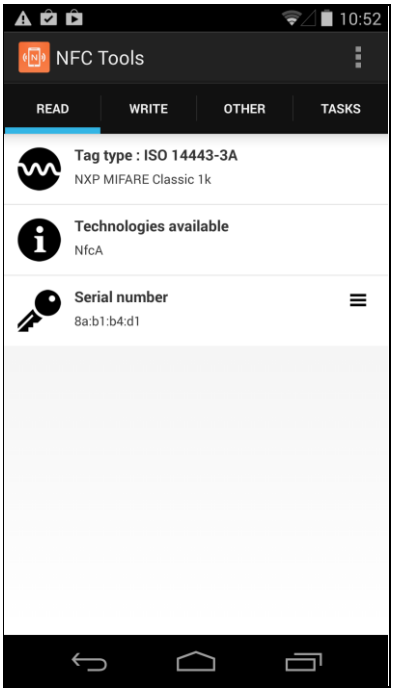


Figura 28 - Código ID NFC do cartão de acesso

Para validar esse requisito funcional, foi instalado no *smartphone* um terminal *bluetooth* (Figura 29), cuja senha é 1234, e o *firmware* foi programado para enviar ao dispositivo pareado, o código NFC lido.

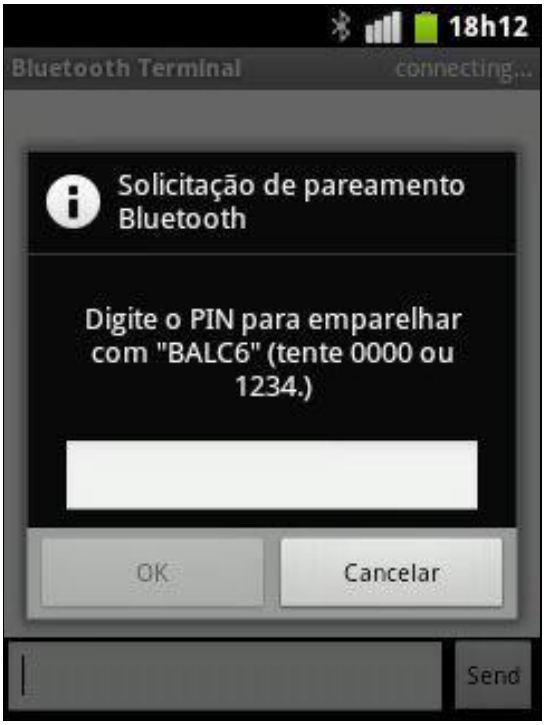


Figura 29 - Pareamento com terminal *Bluetooth*

As Figuras 30 e 31 mostram respectivamente a leitura do cartão genérico e a tela do *smartphone* com o código recebido.

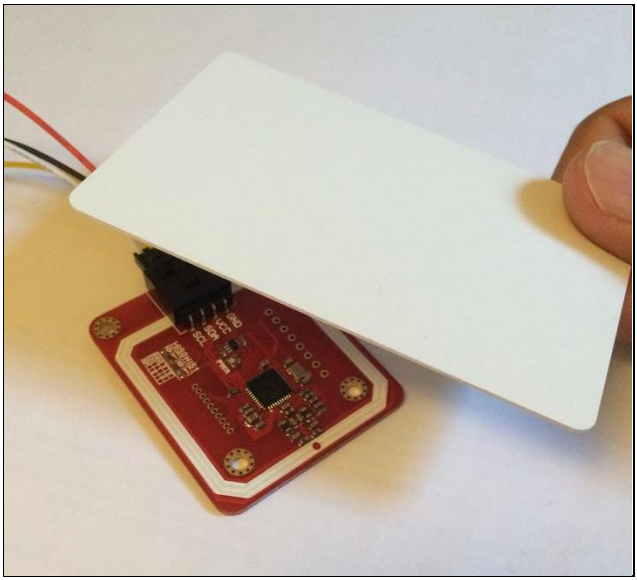

Figura 30 - Leitura do cartão genérico NFC


Figura 31 - Envio do código NFC

Ao fim deste teste foram validadas duas funcionalidades, sendo elas a leitura do código NFC e o envio do ID, via *bluetooth*, para o dispositivo pareado.

### 4.2.3 Recebimento da Permissão

O segundo teste realizado foi o recebimento da resposta do MCA, informando se o usuário possui, ou não, permissão de acesso. Assim como no teste anterior foi utilizado o terminal *bluetooth* para simular o MCA, que retorna o valor 0 (zero) em caso de acesso negado ou 1 (um) para acesso permitido, conforme as Figuras 32 e 33.


Figura 32 - Retorno de acesso permitido do MCA para o MAF


Figura 33 - Retorno de acesso negado do MCA para o MAF

Para cada ação do MAF são acionados o LED e o BUZZER de acordo com a Tabela 5, informando se o acesso foi negado caso receba 0 (zero), ou permitido caso receba 1 (um). As Figuras 34 e 35 mostram, respectivamente, uma situação em que o acesso solicitado foi permitido, acendendo o LED na cor verde, noutra negado, acendo o LED na cor vermelha e o BUZZER, para fins de visualização, está representado pelo LED de cor amarela.

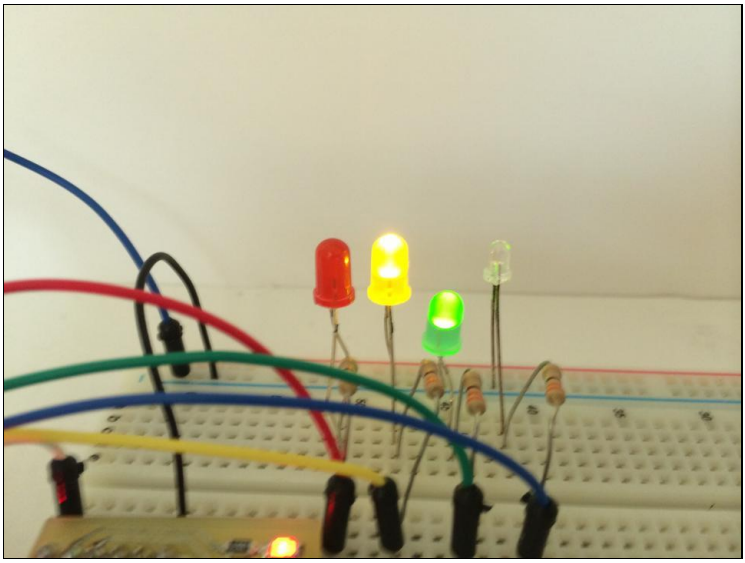

Figura 34 - Feedback de acesso permitido

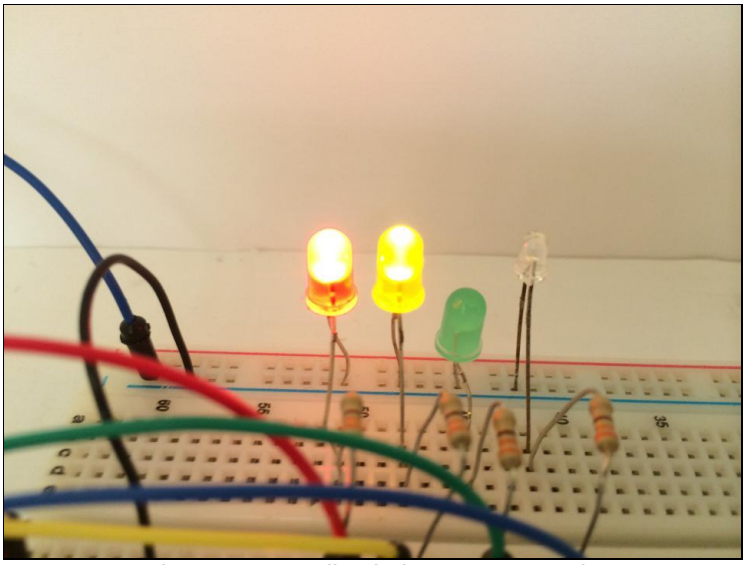

Figura 35 - Feedback de acesso negado

Os testes de permissão foram realizados em outro momento e estão documentados em detalhes a seguir, na Seção de testes funcionais.

### 4.2.4 *Feedbacks* Visuais

Assim que recebe a resposta de permissão de acesso vindo do MCA, o MAF realiza, ou não, o acionamento da fechadura e emite ao usuário feedbacks visuais e sonoros referente a ação realizada pelo módulo. Os *feedbacks* de acesso permitido e negado foram testados na Seção 4.2.2, restando apenas o estado de *stand by* que é representado por um LED constantemente ligado na cor azul, com o intuito de informar ao usuário que o MAF está funcionando. Neste teste foi analisado o comportamento desse LED que se manteve na cor azul (Figura 36) enquanto o MAF não era acionado e retornando ao estado de *stand by* após uma ação de acesso negado ou permitido.

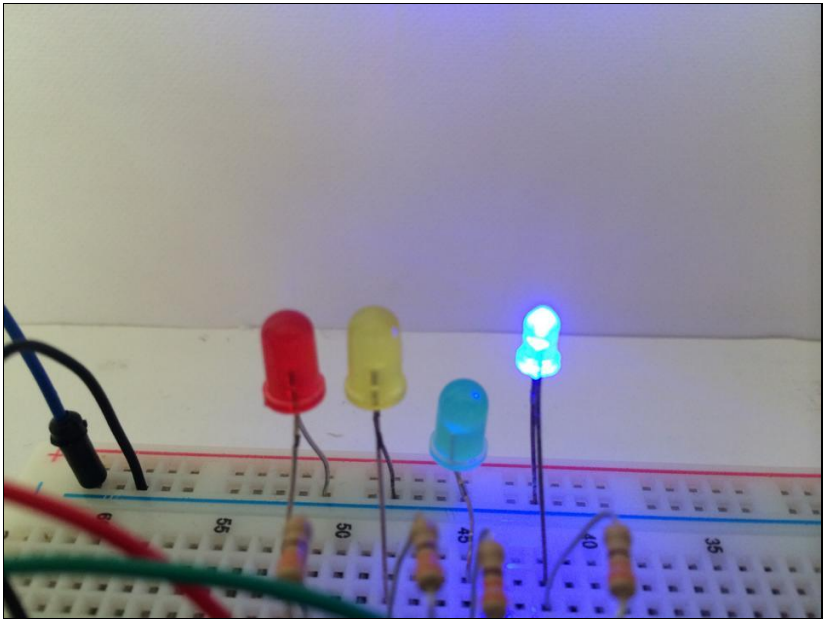


Figura 36 - Estado stand by

## 4.3 TESTES FUNCIONAIS

A Seção anterior enfatizou os testes unitários, ou seja, testar individualmente cada etapa do processo que engloba as fases de leitura, solicitação, consulta de permissão e acionamento da fechadura.

Esta Seção da ênfase aos testes funcionais que consistiu em deixar o MAF em funcionamento, no qual o módulo foi frequentemente acionado durante este período. O MAF e o MCA foram posicionados a uma distância de aproximadamente 7 metros, com a ausência de obstáculos entre os módulos, visando simular um ambiente real de um quarto de hotel.

Neste cenário, foi atribuída a permissão de acesso ao *smartphone* LG Nexus 5, sendo que o mesmo não ocorreu para o cartão genérico NFC. Durante 24 horas, o MAF foi submetido a 50 testes em que o acesso foi permitido, usando o LG Nexus 5, e a mesma quantidade de testes para casos em que o acesso foi negado, usando o cartão NFC genérico. No decorrer dos testes foi calculado o tempo de resposta, que engloba a leitura do ID NFC, a consulta da permissão de acesso, o retorno do MCA e o acionamento, que teve um valor médio de 0,97 segundos. No decorrer deste período o MAF permaneceu estável, respondendo corretamente às solicitações e não apresentou travamento.

# 5 CONCLUSÃO

Esse trabalho apresentou as etapas de concepção, definição, planejamento e execução do projeto que visa o desenvolvimento de um módulo de acionamento da fechadura, que é parte de um projeto de automação para área hoteleira, proposto por professores pesquisadores do GECAD, Grupo de Investigação em Engenharia do Conhecimento e Apoio à Decisão do ISEP, localizado na cidade do Porto. No Capítulo 2, Revisão Bibliográfica, foram apresentados alguns modelos de fechaduras modernas, assim como o estudo realizado com o intuito de definir a tecnologia a ser utilizada para realizar a comunicação entre o módulo de acionamento da fechadura e o controlador central do quarto de hotel. Essa revisão foi fundamental no levantamento das informações necessárias para definir os requisitos funcionais do MAF.

Conforme foi apresentado na Seção 2.1.5, foi realizado um estudo comparativo entre as tecnologias *bluetooth* e *zigbee*, visando definir, de acordo com o cenário de aplicação, a tecnologia mais apropriada para a solução. Por apresentar um melhor rendimento foi decidido utilizar o bluetooth 4.0, porém, por questões de disponibilidade, foi utilizado um módulo com a versão 3.0 da tecnologia e devido a essa mudança a análise do rendimento e autonomia, características essenciais para a solução, ficou comprometida,

Além da versão do *bluetooth*, podem ser citados outros fatores que contribuíram negativamente no desenvolvimento do projeto como, por exemplo, a demora na disponibilização do módulo *bluetooth*, que acarretou em um atraso na implementação do *firmware*. A fechadura utilizada aparentava sinais de uso e desmontagens, o que pode ser a causa da mesma apresentar instabilidade no seu funcionamento mesmo com o *hardware* de fábrica. O fato da fechadura não estar em perfeito estado de funcionamento e a falta de documentação técnica acarretou na substituição da fechadura por um relé, para fins de validação da solução, indicando que o módulo atende às especificações e está preparado para acionar qualquer elemento externo à ele conectado, salvo algumas alterações particulares de *firmware* e *hardware*.

Vale lembrar que o objetivo do trabalho foi desenvolver um protótipo para fins de validação de conceito e uma vez constatado o funcionamento, o projeto sofrerá alterações para que o tamanho do hardware se adeque ao cenário de aplicação da solução. Isso implica em questões de layout, que neste trabalho foi desenhado para a montagem do protótipo considerando a utilização dos módulos PN532 (NFC) e HC-05 (*bluetooth*), porém é inviável ter um produto comercial que contém partes essenciais da solução dependentes de terceiros sem que haja um contrato preestabelecido que garanta o fornecimento dos módulos. Por esses motivos a PCI não foi montada, entretanto deu-se início à construção do layout visando adiantar essa etapa do projeto que certamente exigirá alterações após ambos os módulos serem incorporados ao produto, originando uma solução totalmente proprietária.

A fechadura Okidokeys que, assim como o MAF, possui NFC e *bluetooth* 4.0, no início do ano de 2014 era comercializada por aproximadamente R$ 400,00 reais. O protótipo do MAF custou aproximadamente R$ 121,10 reais (exceto mão-de-obra e a fechadura), tal valor pode ser diminuído em caso de produção em escala e caso seja incorporada à solução os módulos NFC e bluetooth. Considerando o cenário descrito é possível aprofundar os estudos sobre a viabilidade de tornar o MAF um produto comercial rentável.

Por fim, pode-se concluir que o protótipo atendeu as expectativas dentro daquilo que lhe foi proposto, incorporando funcionalidades de modelos comerciais de fechaduras sem desprezar as particularidades impostas pela solução, respondendo bem aos testes no qual foi submetido, dando condições para a continuidade no desenvolvimento e aprimoramento do projeto, visando torna-lo uma solução comercial.

## 5.1 TRABALHOS FUTUROS

Seguem abaixo algumas sugestões de trabalhos futuros relacionados à solução geral, na qual o MAF está incorporado:

- Incorporar o módulo *bluetooth* ao MAF;
- Incorporar o módulo NFC ao MAF;
- Desenvolver um aplicativo para *smartphone* com o objetivo de acionar e controlar os recursos de um quarto de hotel;
- Desenvolver um *software* de gerenciamento de todos os quartos do hotel;
- Criar servidores de serviços internos e externos e
- Desenvolver o módulo de controle e acionamento dos periféricos do quarto de hotel.

# 6 REFERÊNCIAS BIBLIOGRÁFICAS


ACEPI. Associação do comércio eletrônico e publicidade interativa, 2013. Disponível em: <www.acepi.pt/artigoDetalhe.php?idArtigo=91401>. Acesso em: 9 mai 2014.

ANDRADE, Nelson; BRITO, Paulo Lucio de; JORGE, Wilson Edson. Hotel: Planejamento e Projeto. 2ª edição. São Paulo: Senac, 2000.

ARDUINO. Arduino Duemilanove. 2009. Disponível em: <arduino.cc/en/Main/arduinoBoardDuemilanove>. Acesso em: 26 jun 2014.

AURESIDE. Conceitos Básicos. Associação Brasileira de Automação Residencial, 2014. Disponivel em: < http://www.aureside.org.br/noticias_recentes/default.asp?file=01.asp&id=358>. Acesso em: 12 mar 2014.

*BLUETOOTH*. Disponível em: <https://www.*bluetooth*.com >. Acesso em 27 mar 2014.

BOLZANI, C. A. M. Residências Inteligentes. 1ª. ed. São Paulo: Livraria da Física, 2004.

BRITO, Edivaldo. O que é NFC?. Site Techtudo, 2012. Disponível em: < http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-nfc.html>. Acesso em: 9 mai 2014.

CLARK, Sarah. Vodafone adds support for barcode loyalty and membership cards to NFC wallet. NFC World, 2014. Disponível em: <www.nfcworld.com/2014/05/08/329021/vodafone-adds-support-barcode-loyalty-membership-cards-nfc-wallet>. Acesso em: 9 mai 2014.

DECUIR, Joe. *Bluetooth* 4.0: Low Energy. *Bluetooth* SIG and IEEE Consumer Eletronics Society, 2010. Disponível em: <http://chapters.comsoc.org/vancouver/BTLER3.pdf>. Acesso em: 11 abr 2014.

ELECHOUSE. 2014. Disponível em: < http://www.elechouse.com/elechouse/index.php?main_page=product_info&cPath=90_93&products_id=2205>. Acesso em: 16 abr 2014.

HECKE, Caroline. Onde e como a tecnologia NFC está sendo aplicada. Site Tecmundo, 2011. Disponível em: <http://www.tecmundo.com.br/nfc/8173-onde-e-como-a-tecnologia-nfc-esta-sendo-aplicada.htm>. Acesso em: 08 mai 2014.

RICHTEL, Matt. KOPYTOFF, Verne G. Smartphones e NFC anunciam o fim da chave de casa e do carro. 2011. Disponível em: <http://tecnologia.terra.com.br/smartphones-e-nfc-anunciam-o-fim-da-chave-de-casa-e-do-carro,93599256184ea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 16 abr 2014.

ROTHMAN, Paula**.** *Bluetooth* 4.0 gasta menos energia e é 17 vezes mais eficiente. Revista Exame, 2010. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/*bluetooth*-4-0-gasta-menos-energia-17-vezes-mais-eficiente-603170>. Acesso em: 27 mar 2014.

SCRUTTON, Alistais. Global lockmaker seeks key to future profits in the cloud. Disponível em: < http://mobile.reuters.com/article/Deals/idUSL4N0GT2Y720130922?irpc=935 >. Acesso em: 15 abr 2014.

KOBAYASHI, Carlos Y. A Tecnologia *Bluetooth* e aplicações, 2004. Disponível em: <http://grenoble.ime.usp.br/movel/monografia_*bluetooth*.pdf>. Acesso em: 27 mar 2014.

LOCKITRON. 2010. Disponível em: <https://lockitron.com>. Acesso em: 11 abr 2014.

NCONTROL. Disponível em: <http://www.ncontrol.com.pt>. Acesso em: 11 abr 2014.

NFC. Disponível em: < http://www.nearfieldcommunication.org>. Acesso em 07 mai 2014.

OKIDOKEYS. 2014. Disponível em: < https://www.okidokeys.com/packages/8-smart-lock.html>. Acesso em 11 abr 2014.

PEF. Disponível em: <http://pef.com.sapo.pt>. Acesso em 10 abr 2014.

REVISTA HOTEIS**.** O desafio atual do setor hoteleiro. 120ª. ed. São Paulo: Edição on-line. Disponivel em: < http://www.revistahoteis.com.br/materias/15-Opiniao/11304-O-desafio-atual-do-setor-hoteleiro>. Acesso em: 25 mar 2014.

SERAFIN, Marco Antonio M. A história da hotelaria no Brasil e no mundo, 2005. Disponível em: < http://www.etur.com.br/conteudocompleto.asp?idconteudo=6144 >. Acesso em 25 mar 2014.

SOUZA, Ramon. Fechadura com NFC permite destrancar portas com seu celular. 2014. Disponível em: <http://www.tecmundo.com.br/seguranca/49043-fechadura-com-nfc-permite-destrancar-portas-com-seu-celular.htm>. Acesso em: 11 abr 2014.

TEV2. Disponível em: < http://static.tev.pt/Imgs/content/page_640/hotel.pdf >. Acesso em 15 abr 2014.

TEXAS INSTRUMENTS. ***Bluetooth*** **low energy versus ZigBee**, 2010. Disponível em: < http://e2e.ti.com/blogs_/b/connecting_wirelessly/archive/2010/03/09/b.aspx>. Acesso em: 10 abr 2014.

UBITAP. About Near Field Communication. Disponível em: < http://www.ubitap.com/whatisnfc >. Acesso em: 12 mai 2014.

XBEESTORE. Disponivel em: <http://www.xbeestore.com.br >. Acesso em: 21 mar 2014.

ZIGBEE. Disponível em: <https://www.zigbee.org>. Acesso em: 27 mar 2014.

# APÊNDICES

# APÊNDICE A – CHECK-LIST DE TESTES UNITÁRIOS

| Teste | Descrição | Resultado | Observações |
|---|---|---|---|
| Leitura do ID NFC | Obter código identificador NFC do smartphone | | |
| Comunicação com MCA (emissão) | Enviar, via *bluetooth*, o ID NFC para o MCA | | |
| Comunicação com MCA (recepção) | Receber do MCA a resposta da solicitação de acesso. | | |
| Acionamento da Fechadura | Abrir a fechadura quando receber a resposta de acesso permitido | | |
| Fechadura em posição padrão | Manter a fechadura trancada até que receba um comando de acionamento. | | |
| Feedback visual: Standby | Manter o LED azul constantemente aceso | | |
| Feedback visual: Acesso permitido | Piscar uma vez o LED verde | | |
| Feedback visual: Acesso negado | Piscar três vezes o LED vermelho | | |
| Feedback sonoro: Standby | Sem som | | |
| Feedback sonoro: Acesso permitido | Emitir um bipe sonoros | | |
| Feedback sonoro: Acesso negado | Emitir três bipes sonoros | | |
| Reconhecimento do Módulo NFC | Manter o LED vermelho aceso constantemente | | |