

Karla Maria Garcia

**SISTEMA DE CONTROLE DE ACESSO VEICULAR
UTILIZANDO TECNOLOGIA RFID**

FLORIANÓPOLIS, 2013

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E
TECNOLOGIA DE SANTA CATARINA
CAMPUS FLORIANÓPOLIS
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE PÓS-GRADUAÇÃO LATO SENSU –
ESPECIALIZAÇÃO EM DESENVOLVIMENTO DE PRODUTOS
ELETRÔNICOS**

KARLA MARIA GARCIA

**SISTEMA DE CONTROLE DE ACESSO VEICULAR
UTILIZANDO TECNOLOGIA RFID**

**Monografia submetida ao Instituto
Federal de Educação, Ciência e
Tecnologia de Santa Catarina
como parte dos requisitos para
obtenção do título de Especialista
em Desenvolvimento de Produtos
Eletrônicos.**

**Professor Orientador: Charles
Borges Lima, Dr. Eng.**

FLORIANÓPOLIS, 2013

CDD 621.382

G216s

Garcia, Karla Maria

Sistema de controle de acesso veicular utilizando tecnologia RFID
[Monografia] / Karla Maria Garcia; orientação de Charles Borges Lima. –
Florianópolis, 2013.

1 v. : il.

Monografia de especialização (Desenvolvimento de Produtos Eletrônicos) –
Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.
Curso de Pós-graduação Lato Sensu em Desenvolvimento de Produtos
Eletrônicos.

Inclui referências.

1. RFID. 2. Microcontrolador. 3. Sistema de identificação – Controle de
acesso. I. Lima, Charles Borges. II. Título.

Sistema de Bibliotecas Integradas do IFSC

Biblioteca Dr. Hercílio Luz – Campus Florianópolis

Catalogado por: Edinei Antonio Moreno CRB 14/1065


SISTEMA DE CONTROLE DE ACESSO VEICULAR UTILIZANDO TECNOLOGIA RFID

Karla Maria Garcia

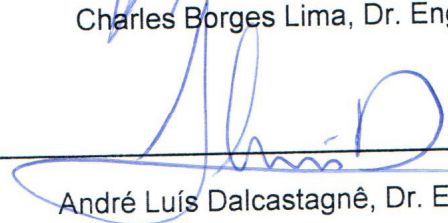
Este trabalho foi julgado adequado para obtenção do Título de Especialista em Desenvolvimento de Produtos Eletrônicos e aprovado na sua forma final pela banca examinadora do Curso de Especialização em Desenvolvimento de Produtos Eletrônicos do Instituto Federal de Educação, Ciência e Tecnologia de Santa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

Florianópolis, 18 de setembro de 2013.

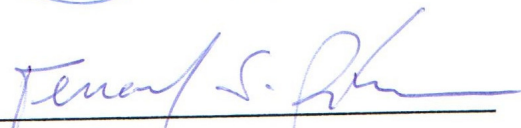
Banca Examinadora:

A handwritten signature in blue ink, appearing to be 'Charles B. Lima', written over a horizontal line.

Charles Borges Lima, Dr. Eng.

A handwritten signature in blue ink, appearing to be 'André Luís Dalcastagnê', written over a horizontal line.

André Luís Dalcastagnê, Dr. Eng.

A handwritten signature in blue ink, appearing to be 'Fernando S. Pacheco', written over a horizontal line.

Fernando Santana Pacheco, Dr. Eng.

AGRADECIMENTOS

Agradeço primeiramente àqueles que são os meus pilares, minha mãe e minha irmã, Lourdes e Kelly, pelo amor e carinho que sempre me deram. Ao meu amado pai, Pedro, que mesmo tendo passado poucos anos comigo, conseguiu me transmitir princípios valiosos. Ao meu marido e melhor amigo, Guilherme, sempre ao meu lado me apoiando e motivando.

A todos os professores que ministraram aulas para a quinta turma da Pós Graduação em Desenvolvimento de Produtos Eletrônicos, pelos conhecimentos transmitidos. Especialmente ao professor Charles Borges Lima por ter se disponibilizado a me ajudar na elaboração deste trabalho.

Aos colegas de trabalho, que me ouviram falar sobre este projeto nos últimos seis meses, e mesmo sem compreender muito sobre o assunto, sempre garantiam que iria dar certo e eu conseguiria concluir.

A todos que contribuíram, direta ou indiretamente, um sincero muito obrigada!

*Não sabendo que era impossível,
ele foi lá e fez.
Jean Cocteau*

RESUMO

Sistemas de identificação automática tornaram-se comuns em soluções para controle de acesso e aplicações de segurança em indústrias que requerem rastreamento de produtos no processo de abastecimento e/ou fabricação. Uma das tecnologias empregadas nesses sistemas é a identificação por radiofrequência (RFID), tecnologia versátil que possibilita a transferência de dados sem necessidade de fios, contato físico ou de uma linha de visada. Considerando as vantagens desta tecnologia, o presente trabalho desenvolveu um sistema para controle de acesso em estacionamentos utilizando RFID. O modelo desenvolvido considerou cenários com duas cancelas, uma de entrada e outra de saída. O modelo se divide em dois módulos: aplicação web e sistema microcontrolado, sendo esse constituído por microcontrolador, display, conector ethernet e servomotores que simulam cancelas. O sistema microcontrolado, desenvolvido em linguagem de programação C, permite ao microcontrolador verificar se as etiquetas RFID apresentadas aos leitores possuem permissão de acesso, movimentar as cancelas e informar no display, localizado na entrada, a quantidade de vagas livres. A aplicação web é utilizada para o usuário efetuar cadastros, edições e consultas de funcionários e veículos, bem como consulta dos acessos inseridos no banco de dados pelo microcontrolador. Um protótipo foi desenvolvido para avaliar a viabilidade do modelo através da execução de testes.

Palavras chaves: RFID, microcontrolador, controle de acesso, embarcado.

ABSTRACT

Automatic identification systems have become common in solutions for access control and security applications in industries that require product tracking in the supply process and/or manufacturing. One of the technologies used in these systems is the radio frequency identification (RFID), versatile technology that enables data transfer without the need for wires, physical contact or line of sight. Considering the advantages of this technology, this study developed a system for access control in parking lots using RFID. The model considered scenarios with two gates, one entrance and one exit. The model is divided into two modules: web application and system microcontroller and this consists of microcontroller, display, ethernet connector and servo motors that simulate gates. The microcontroller checks if the RFID tags presented to the readers have access permission, moves the gates and shows in the display, located at the entrance, the amount of free spaces. The web application is used to register, edit and consult employees and vehicles, as well as to query the registers of access entered into the database by the microcontroller. A prototype was developed to evaluate the feasibility of the model by running tests.

Keywords: RFID, microcontroller, access control, embedded.

LISTA DE ILUSTRAÇÕES

<i>FIGURA 2.1 - Componentes de Sistema RFID.....</i>	<i>30</i>
<i>FIGURA 2.2 - Arquitetura de sistema RFID.....</i>	<i>32</i>
<i>FIGURA 2.3 – Exemplo de layout básico de uma etiqueta.</i>	<i>34</i>
<i>FIGURA 2.4 - Exemplos de etiquetas passivas.</i>	<i>36</i>
<i>FIGURA 2.5 - Exemplos de etiquetas semi-passivas e ativas.....</i>	<i>38</i>
<i>FIGURA 2.6 - Fluxo de dados entre aplicação, leitor e etiqueta.....</i>	<i>40</i>
<i>FIGURA 2.7 - Componentes principais do leitor.</i>	<i>41</i>
<i>FIGURA 3.1 - Modelo do sistema de controle de acesso.....</i>	<i>55</i>
<i>FIGURA 3.2 - Estacionamento com controle de acesso.....</i>	<i>56</i>
<i>FIGURA 3.3 – Fluxograma do procedimento de inicialização do sistema microcontrolado.</i>	<i>58</i>
<i>FIGURA 3.4 - Fluxograma do procedimento de entrada.</i>	<i>60</i>
<i>FIGURA 3.5 - Fluxograma do procedimento de saída.</i>	<i>61</i>
<i>FIGURA 3.6 - Placa de desenvolvimento ARM mbed NXP LPC1768.</i>	<i>63</i>
<i>FIGURA 3.7 - ID-12 Innovations.....</i>	<i>65</i>
<i>FIGURA 3.8 - Placa adaptadora do leitor RFID.</i>	<i>66</i>
<i>FIGURA 3.9 - Etiqueta RFID.</i>	<i>67</i>
<i>FIGURA 3.10 - Módulo MicroSD.....</i>	<i>68</i>
<i>FIGURA 3.11 - Micro Servomotor.....</i>	<i>69</i>
<i>FIGURA 4.1 - Interface de desenvolvimento.</i>	<i>72</i>
<i>FIGURA 4.2 - Modelo lógico da base de dados.....</i>	<i>75</i>
<i>FIGURA 4.3 - Sistema de Controle de Estacionamento RFID - Tela Principal.....</i>	<i>76</i>
<i>FIGURA 4.4 - Tela para Cadastro de Funcionário.....</i>	<i>76</i>
<i>FIGURA 4.5 – Tela para Listar Funcionários.....</i>	<i>77</i>
<i>FIGURA 4.6 – Tela para Cadastro de Veículos.</i>	<i>77</i>
<i>FIGURA 4.7 - Tela para Listar Veículos.</i>	<i>78</i>
<i>FIGURA 4.8 - Tela para Listar Registros.....</i>	<i>78</i>
<i>FIGURA 4.9 - Tela Relação de Registros de Acesso.....</i>	<i>79</i>
<i>FIGURA 4.10 - Dispositivos auxiliares ao microcontrolador.....</i>	<i>79</i>
<i>FIGURA 4.11 - Arquivos do sistema de controle RFID.....</i>	<i>82</i>

<i>FIGURA 4.12 – Conteúdo do arquivo persistencia.h.....</i>	<i>83</i>
<i>FIGURA 4.13 - Conteúdo do arquivo display.h.</i>	<i>83</i>
<i>FIGURA 4.14 - Conteúdo do arquivo cancela.h.</i>	<i>84</i>
<i>FIGURA 4.15 - Conteúdo do arquivo conexao_bd.h.</i>	<i>85</i>
<i>FIGURA 4.16 - Conteúdo do arquivo controle_rfid.h.</i>	<i>86</i>
<i>FIGURA 4.17 – Interligação do microcontrolador ao SDcard, ethernet e display.....</i>	<i>87</i>
<i>FIGURA 4.18 – Interligação do microcontrolador aos servomotores e leitores RFID</i>	<i>88</i>
<i>FIGURA 4.19 - Layout do projeto.</i>	<i>89</i>
<i>FIGURA 4.20 – Protótipo desenvolvido.....</i>	<i>90</i>
<i>FIGURA 5.3 - Display informando acesso não autorizado.</i>	<i>94</i>
<i>FIGURA 5.4 - Display informando LOTADO.....</i>	<i>95</i>
<i>FIGURA 5.5 - Registro de falha na entrada.</i>	<i>95</i>
<i>FIGURA 5.6 - Registro de saída.....</i>	<i>96</i>
<i>FIGURA 5.7 - Registros de entrada e saída</i>	<i>96</i>

LISTA DE TABELAS

<i>TABELA 2.1 - Comparação entre etiquetas ativas e passivas.</i>	<i>39</i>
<i>TABELA 2.2 - Comparativo entre frequências RFID.</i>	<i>47</i>
<i>TABELA 3.1 - Periféricos mbed NXP-1768.</i>	<i>64</i>
<i>TABELA 3.2 - Características leitor RFID.</i>	<i>66</i>
<i>TABELA 3.3 - Características da etiqueta RFID empregada.</i>	<i>67</i>
<i>TABELA 4.1 - Principais custos de hardware do projeto.</i>	<i>92</i>

LISTA DE ABREVIATURAS E SIGLAS

ABA	<i>American Bankers Association</i>
AIAG	<i>Automotive Industry Action Group</i>
ADSL	<i>Asymmetric Digital Subscriber Line</i>
ANATEL	<i>Agência Nacional de Telecomunicações</i>
API	<i>Application Programming Interface</i>
ARES	<i>Advanced Routing and Editing Software</i>
ARM	<i>Advanced Risc Machine</i>
ASK	<i>Amplitude Shift Keying</i>
Auto-ID	<i>Automatic Identification</i>
CAN	<i>Controller-Area Network</i>
DIP	<i>Dual in-line Package</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>
EAN	<i>European Article Number Association</i>
EAS	<i>Electronic Article Surveillance</i>
EDA	<i>Electronic Design Automation</i>
EDI	<i>Electronic Data Interchange</i>
EEPROM ...	<i>Electrically-Erasable Programmable Read-Only Memory</i>
EPC	<i>Electronic Product Code</i>
FK	<i>Foreign Key</i>
GSMP	<i>Global Standard Management Process</i>
HTML	<i>HyperText Markup Language</i>
I2C	<i>Inter-Integrated Circuit</i>
ID	<i>Identificador</i>
IDE	<i>Integrated Development Environment</i>
IEC	<i>International Electrotechnical Commission</i>
IP	<i>Internet Protocol</i>
ISIS	<i>Intelligent Schematic Input System</i>
ISM	<i>Industrial, Scientific and Medical</i>
ISO	<i>International Standards Organization</i>
ITU-T	<i>International Telecommunication Union - Telecommunication Standardization Sector</i>
JT ₁	<i>Joint Technical Committee 1</i>
LCD	<i>Liquid Crystal Display</i>
PHP	<i>Personal Home Page</i>

PWM	<i>Pulse-Width Modulation</i>
RAM	<i>Random Access Memory</i>
RF	<i>Radio Frequency</i>
RFID	<i>Radio Frequency Identification</i>
RTLS	<i>Real Time Locating System</i>
SD Card	<i>Secure Digital Card</i>
SNMP	<i>Simple Network Management Protocol</i>
SPI	<i>Serial Port Interface</i>
SQL	<i>Structured Query Language</i>
TDMA	<i>Time Division Multiple Access</i>
UCC	<i>Universal Code Council</i>
USB	<i>Universal Serial Bus</i>
WG3	<i>Workgroup 3</i>
WG4	<i>Workgroup 4</i>
XML	<i>eXtensible Markup Language</i>

SUMÁRIO

1.	INTRODUÇÃO.....	23
1.1	DEFINIÇÃO DO PROBLEMA	24
1.2	OBJETIVOS	25
1.2.1	<i>Objetivo geral.....</i>	<i>25</i>
1.2.2	<i>Objetivos específicos</i>	<i>25</i>
1.3	JUSTIFICATIVA	26
1.4	ESTRUTURA DO TRABALHO	26
2.	TECNOLOGIA DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (RFID) .	29
2.1	PRINCÍPIO DE FUNCIONAMENTO	29
2.2	COMPONENTES BÁSICOS.....	33
2.2.1	<i>Etiquetas.....</i>	<i>33</i>
2.2.2	<i>Leitores</i>	<i>39</i>
2.3	TERMOS TÉCNICOS	44
2.4	FREQUÊNCIA DE OPERAÇÃO	45
2.5	PADRONIZAÇÃO	48
3.	MODELO PARA CONTROLE DE ACESSO EM ESTACIONAMENTOS ...	53
3.1.	DEFINIÇÃO	53
3.2.	SISTEMA MICROCONTROLADO	55
3.3.	APLICAÇÃO WEB	61
3.4.	ESPECIFICAÇÃO DOS DISPOSITIVOS UTILIZADOS	62
4.	IMPLEMENTAÇÃO DA ARQUITETURA	71
4.1	FERRAMENTAS UTILIZADAS	71
4.2	DESCRIÇÃO DO SOFTWARE.....	74
4.3	DESCRIÇÃO DO HARDWARE.....	87
4.4	CUSTOS DO PROJETO	91
5.	TESTES REALIZADOS E RESULTADOS	93
6.	CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS.....	99

REFERÊNCIAS.....	101
APÊNDICES	105
APÊNDICE A – SQLS PARA CRIAÇÃO DAS TABELAS DE DADOS	107

1. INTRODUÇÃO

O avanço tecnológico na busca por eficiência e eficácia na execução de processos converge para a automação de sistemas. A adoção de sistemas automatizados proporciona maior segurança, conforto, agilidade, economia e possui a vantagem de que praticamente qualquer atividade pode ser parcial ou completamente automatizada. A popularização da automação tornou-se possível devido ao desenvolvimento da eletrônica, e consequente redução de custos, que permitiu a elaboração de dispositivos digitais cada vez menores e mais eficientes.

Sistemas de identificação automática (Auto-ID) têm por objetivo fornecer informações sobre pessoas, animais e objetos. A revolução nos sistemas de identificação iniciou com os códigos de barra. Todavia, apesar de serem extremamente acessíveis (baixo custo) quando comparados às demais tecnologias, estão se tornando obsoletos devido à baixa capacidade de armazenamento e a impossibilidade de reprogramação. Os *smarts cards* também são uma opção em soluções de identificação, entretanto, em determinados casos, a necessidade de contato para a transferência dos dados inviabiliza o seu uso. A identificação por radiofrequência (RFID) tem a vantagem de possibilitar operações de captura e identificação automática de dados, sem que haja contato físico (FINKENZELLER, 2010).

A RFID foi empregada pela primeira vez durante a Segunda Guerra Mundial, quando alemães utilizaram um aparelho eletrônico que permitia transmitir um código de identificação e, assim, distinguir os aviões aliados dos demais. Segundo PALA e INANÇ (2007), apesar de já ter sido desenvolvida há algumas décadas, por um longo período de tempo ela não foi amplamente explorada devido ao alto custo e pelo fato de não existir uma padronização entre as empresas desenvolvedoras. Entretanto, conforme Sharma e Siddiqui (2010), o interesse pela RFID cresceu exponencialmente nos últimos anos, sendo que esse crescimento, principalmente na área logística, fez reduzir os preços dos componentes (etiquetas e leitores) e, consequentemente, abriu possibilidades para outros

campos de negócios se beneficiarem das vantagens dessa tecnologia.

Especialistas preveem que a RFID irá revolucionar áreas da indústria, como a gestão da cadeia de suprimentos e os negócios de varejo, reduzindo custos através de um melhor gerenciamento do estoque (SHARMA e SIDDIQUI, 2010).

Conforme GAO RFID Inc (2013), devido à necessidade de maior segurança para limitar acesso a áreas restritas, controle das atividades de colaboradores e reduzir a possibilidade de roubos, muitas organizações requerem sistemas de controle de acesso. Considerando a demanda por sistemas de controle de acesso e que essas soluções podem ser implementadas de forma simples através de sistemas embarcados, o presente trabalho tem por objetivo elaborar um protótipo para gerenciamento de acesso de automóveis a estacionamentos. É proposto um sistema embarcado a fim de efetuar de forma dedicada o controle de entrada/saída de veículos, via reconhecimento de etiquetas e da quantidade de vagas livres. O usuário irá apresentar sua etiqueta na portaria do estacionamento e sua permissão de acesso será verificada. Em caso positivo, o portão será aberto. Os registros serão armazenados em cartões de memória, ficando disponíveis para consultas posteriores.

1.1 Definição do problema

Por razões de segurança, instituições como empresas, escolas e condomínios passaram a controlar o acesso de veículos aos seus estacionamentos. Geralmente, esse controle é realizado por um indivíduo que fica responsável pela identificação dos veículos, o que torna o sistema suscetível a erros humanos. Além do problema com a identificação das pessoas autorizadas, há a dificuldade em controlar a quantidade de vagas disponíveis. Por falhas na contagem dos carros que entram e saem do local, ocorrem situações em que sobram vagas e outras em que uma quantidade de automóveis superior à

capacidade do estacionamento é autorizada a entrar, gerando desconforto aos usuários.

1.2 Objetivos

1.2.1 Objetivo geral

Desenvolvimento de um sistema para gerenciamento de estacionamentos utilizando a tecnologia RFID.

1.2.2 Objetivos específicos

- Definir um modelo para o controle de acesso a ser realizado.
- Desenvolver uma estrutura de hardware para integrar leitores RFID, microcontrolador, cartão de memória, servomotor e *display*.
- Implementar um software embarcado para efetuar o controle de acesso e o gerenciamento da quantidade de vagas, utilizando a tecnologia RFID.
- Apresentar em um *display* a quantidade de vagas disponíveis.
- Efetuar o controle de servomotores simulando o acionamento de cancelas.
- Desenvolver uma aplicação web que permita ao usuário do sistema cadastrar funcionários, veículos e consultar registros de acesso.

1.3 Justificativa

Muitas instituições ainda adotam sistemas manuais para o controle de acesso e de monitoramento dos veículos em seus estacionamentos e, conseqüentemente, enfrentam problemas decorrentes de erros humanos. A automatização do controle de acesso a estacionamentos é uma solução vantajosa, pois evita problemas com acesso não autorizado, mau aproveitamento das vagas e estacionamentos indevidos, além de disponibilizar em tempo real informação sobre a quantidade de vagas livres e permitir consultar quais usuários acessaram o estacionamento em determinado período.

1.4 Estrutura do trabalho

Este trabalho é composto por seis capítulos, organizados conforme descrito a seguir.

Capítulo 2: Tecnologia de identificação por radiofrequência

Inicialmente, descreve-se o funcionamento de sistemas RFID básicos. Em seguida apresentam-se as características mais importantes de leitores/etiquetas e as frequências disponíveis para operação. O capítulo é finalizado citando os principais padrões e órgãos reguladores.

Capítulo 3: Arquitetura para controle de acesso em estacionamentos

É descrita a arquitetura desenvolvida com a finalidade de possibilitar o controle de estacionamentos utilizando RFID e os dispositivos escolhidos para implementar o sistema.

Capítulo 4: Implementação da Arquitetura

São apresentados os detalhes de implementação do modelo proposto, bem como as ferramentas utilizadas no seu desenvolvimento.

Capítulo 5: Testes realizados e resultados

São apresentados os testes executados com o protótipo a fim de confirmar se os objetivos propostos foram alcançados.

Capítulo 6: Conclusões e sugestões para trabalhos futuros

Conclui-se o trabalho ressaltando-se os benefícios alcançados com a solução proposta e apresentando possíveis melhorias no modelo implementado.

2. TECNOLOGIA DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (RFID)

A tecnologia da informação é amplamente reconhecida como um importante fator para a transformação dos negócios e o crescimento econômico. Os principais exemplos de inovação são encontrados em situações nas quais a criação e a aplicação de tecnologias da informação fornecem conectividade aberta e onipresente. Notebooks, celulares e a Internet são exemplos de tecnologias da informação que se tornaram onipresentes. A identificação por radiofrequência é uma inovação tecnológica emergente e algumas comunidades acadêmicas e profissionais arriscam dizer que ela será responsável por uma revolução na cadeia de suprimentos, através da gestão de estoques e *check-out* de produtos, por exemplo (WANBA et. al., 2009).

Conforme Haver (2006), a identificação por radiofrequência é um termo genérico para tecnologias que transmitem a identidade de um objeto, ou entidade, a partir de uma etiqueta para um leitor por meio de ondas de radiofrequência. A RFID não é uma tecnologia nova, porém inicialmente seu custo inviabilizava sua adoção. Entretanto, o desenvolvimento de técnicas de produção proporcionou uma redução substancial no custo dos sistemas baseados nessa tecnologia, tornando-os viáveis para uma ampla gama de aplicações.

2.1 Princípio de funcionamento

Segundo Pedro (2008), um sistema RFID é composto, basicamente, pelos seguintes componentes:

- Etiqueta – constituída por um pequeno *microchip* equipado com uma antena (*transponder* – *transmitter/responder*) e por um invólucro.

- Leitor – referenciado em algumas literaturas como interrogador ou *transceiver* (*transmitter/receiver*), é constituído pelo próprio leitor e uma antena.
- Sistema de recolhimento de dados – para onde os dados são enviados e tratados.

Na Figura 2.1 é representada a integração entre esses componentes.

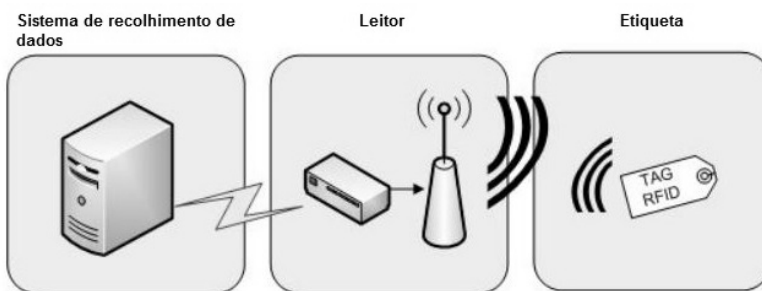


FIGURA 2.1 - Componentes de Sistema RFID.

Fonte: PEDRO, 2008, p. 20.

O *microchip* que compõe a etiqueta é constituído por uma memória para armazenamento de dados e uma unidade lógica responsável pela implementação do protocolo de comunicação entre a etiqueta e o leitor. O tamanho do *microchip* é muito menor que o da antena, logo é esta que determina o tamanho das etiquetas (GOMES, 2007).

Há diversas formas de identificar objetos utilizando RFID, porém a mais comum é armazenar na memória interna da etiqueta um número serial que distingue o produto. Em um sistema RFID básico, o leitor irá emitir uma onda de rádio que será recebida por uma etiqueta compatível. Consequentemente, a etiqueta irá responder com outra onda de rádio que portará a

sua identidade. Após obter a identificação, o leitor envia essa informação para o sistema de recolhimento de dados que é responsável por processá-la. O meio utilizado para a transferência das informações entre o leitor e o sistema de recolhimento de dados depende da interface de comunicação do leitor (PEDRO, 2008).

Segundo Lahiri (2005), sistemas RFID são caracterizados quanto ao método de acoplamento físico, que se refere à forma como é realizado o acoplamento entre a etiqueta e a antena do leitor, ou seja, o mecanismo pelo qual a energia é transferida da etiqueta para a antena do leitor. Baseado neste critério, sistemas RFID podem ser classificados em três tipos diferentes:

- Magnético: são também conhecidos como sistemas de acoplamento indutivo.
- Elétrico: são também conhecidos como sistemas de acoplamento capacitivo.
- Eletromagnético: a maioria dos sistemas de RFID que pertencem a essa classe são também conhecidos como sistemas *backscatter*.

Sistemas RFID operando em altas e baixas frequências podem utilizar tanto mecanismos magnéticos como elétricos para a transmissão de dados. Entretanto, sistemas operando nas faixas de frequência ultra altas e microondas fazem uso de mecanismos eletromagnéticos.

A tecnologia RFID supera as limitações de outros sistemas de identificação automática que utilizam feixes de luz para comunicação, como códigos de barras e tecnologia infravermelhos. Por utilizar ondas de rádio a RFID não exige uma linha de comunicação visada, permitindo que etiquetas fiquem ocultas podendo ser usadas em ambientes hostis e sujos. Os leitores podem ser configurados para lerem remotamente e automaticamente sem necessidade de intervenção frequente (QAISER e KHAN, 2006).

Pedro (2008) apresenta uma arquitetura de referência para sistemas RFID que se divide em três grupos: hardware, interface de borda e software, conforme a Figura 2.2.

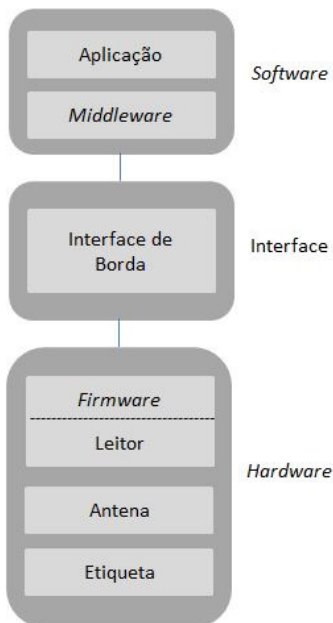


FIGURA 2.2 - Arquitetura de sistema RFID.

Fonte: PEDRO, 2008, p. 21.

No grupo do hardware estão os dispositivos físicos: etiqueta, antena, leitor e *firmware*. Este último é utilizado por dispositivos externos para controlar o leitor. A interface de borda é responsável pela integração entre os grupos de *hardware* e *software*, funcionando como uma camada de abstração que possibilita à aplicação utilizar o hardware sem precisar conhecer detalhes de configuração do leitor. A interface permite que a informação obtida pelo leitor seja transferida para uma camada superior especializada no processamento dos dados. O grupo de *software* representa o sistema de recolhimento de dados, o qual pode ser dividido entre a aplicação e o *middleware*, que atua também como uma camada de abstração responsável pela

comunicação entre a interface de borda e a aplicação que irá utilizar a informação obtida com o sistema RFID.

A arquitetura em camadas permite ao desenvolvedor focar no domínio do negócio de seu projeto, podendo abstrair detalhes de implementação relacionados à identificação por radiofrequência. É possível efetuar o desenvolvimento de soluções RFID sem adotar uma arquitetura em camadas, porém isso dificulta a reutilização do código e suas futuras manutenções.

2.2 Componentes Básicos

Nesta seção, são abordados mais detalhadamente dois principais dispositivos de sistemas RFID, as etiquetas e os leitores.

2.2.1 Etiquetas

Segundo Haver (2006), a etiqueta é basicamente um *microchip* que transporta informação, tanto recebendo como enviando sinal, e uma resistência atuando como antena, ambos envoltos por um material de plástico ou silicone. Geralmente, é gravada no *microchip* a identidade do objeto associado, porém outras informações também podem ser armazenadas. As etiquetas podem incorporar baterias, microprocessadores e memórias EEPROM (*Electrically-Erasable Programmable Read-Only Memory*), que permitem ampliar a capacidade de armazenamento. A memória pode ser dividida em um setor de memória geral e um setor de memória seguro. O setor de memória geral está disponível para leitores, ao passo que o setor de memória seguro é usado para armazenar chaves e normalmente não está disponível para os leitores. O *layout* básico de uma etiqueta é representado na Figura 2.3.

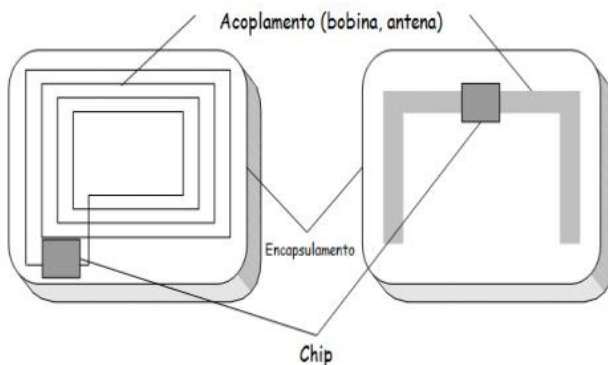


FIGURA 2.3 – Exemplo de *layout* básico de uma etiqueta.

Fonte: FINKENZELLER, 2010, p. 8.

Conforme Radio-Electronics (2013), a fim de padronizar as etiquetas RFID, a instituição *Auto-ID Center*¹ as dividiu em seis classes:

- Classe 0: etiquetas passivas, somente para leitura, seu microchip é gravado no momento em que são produzidas.
- Classe 1: etiquetas passivas, somente para leitura, que permitem programação não volátil uma única vez.
- Classe 2: etiquetas passivas com memória de leitura e escrita de até 65 kB.
- Classe 3: etiquetas semi-passivas com memória de leitura e escrita de até 65 kB e bateria incorporada para proporcionar maior alcance de leitura.

¹ O *Auto-ID Center* é uma organização internacional de pesquisa sem fins lucrativos, fundada em 1999 e sediada no Instituto de Tecnologia de Massachusetts. Tem como missão projetar a infraestrutura e desenvolver normas para criar uma rede universal e aberta para identificação individual de produtos, sendo possível segui-los à medida que percorrem a cadeia de abastecimento global.

- Classe 4: etiquetas ativas que possuem bateria para permitir funcionalidades extras e efetuar a transmissão de informações.
- Classe 5: etiquetas ativas com circuitos adicionais que permitem comunicação com as outras cinco classes.

Conforme verificado na classificação supracitada, existem três tipos de etiquetas: ativas, semi-passivas e passivas.

Etiquetas passivas

Conforme NAEC et al. (2006), as etiquetas passivas classes 0 e 1 não possuem bateria, são menores, possuem alcance de leitura relativamente mais curto do que as etiquetas ativas (em função da frequência), apresentam menor custo e não necessitam de manutenção, razões pelas quais são mais empregadas em cadeias de suprimentos.

Etiquetas passivas apresentam como desvantagens a baixa capacidade de armazenar informações, a considerável sensibilidade a interferências do meio e ausência de uma fonte de alimentação própria. Por não possuírem bateria, a energia necessária para transmissão de dados é obtida através do sinal enviado pelo leitor, exigindo que este tenha mais potência. As etiquetas passivas operam no modo de funcionamento conhecido como *backscatter*, ou seja, quando as etiquetas estão fora da zona de alcance de um leitor elas não possuem nenhuma fonte de alimentação. Logo, não são capazes de emitir sinais, sendo ativadas somente no momento em que recebem as ondas de radiofrequência utilizando essa energia para alimentar seus circuitos e enviar os dados ao leitor (PEDRO, 2008).

Conforme a Figura 2.4, o *transponder* pode ser encapsulado de diferentes formas. Ele pode ser montado sobre um substrato para criar uma etiqueta ou ser colocado entre uma camada adesiva e um rótulo de papel para criar uma etiqueta RFID impressa ou *smart label*. O *transponder* também pode ser incorporado em cartões de plástico, porta chaves e embalagens

especiais para resistir ao calor, frio ou produtos químicos de limpeza. A forma e o material utilizado dependem da aplicação para a qual as etiquetas serão empregadas, porém, o invólucro aumenta significativamente o custo da etiqueta (NAEC et al., 2006).



FIGURA 2.4 - Exemplos de etiquetas passivas.

Etiquetas ativas

Conforme Pedro (2008), etiquetas ativas são caracterizadas por possuírem uma fonte de energia própria para alimentar seus circuitos, tornando o início do processo de transmissão independente das ondas de radiofrequência emitidas pelo leitor. A bateria também possibilita que a etiqueta suporte memórias com maior capacidade de armazenamento e efetue outras funções como monitoramento e controle. A antena pode ter dimensões menores em relação às etiquetas passivas e geralmente são embutidas no módulo de radiofrequência (RF).

De acordo com NAEC et al. (2006), empregam-se etiquetas ativas no rastreamento de objetos de grande valor ao longo de grandes distâncias como, por exemplo, contêineres e caminhões. São utilizadas na maioria dos sistemas de localização em tempo real (RTLS, em inglês *Real-time locating systems*), onde a localização exata de um objeto precisa ser rastreada. Em um RTLS, a etiqueta emite um sinal com o seu identificador em intervalos pré-definidos. O sinal é captado por pelo menos três antenas de leitores posicionados ao redor do perímetro da área onde é feita a monitoração. RTLS são

normalmente utilizados em ambientes externos como, por exemplo, pátios de distribuição. Porém, as montadoras usam os sistemas em grandes fábricas para rastrear caixas de peças.

Sistemas ativos geralmente apresentam um desempenho melhor do que os sistemas passivos quando atuam em ambientes com muitos materiais metálicos e em condições meteorológicas difíceis. Etiquetas ativas, por possuírem uma fonte de energia local, podem ser expandidas através de ampliação de memória e capacidade de processamento. Elas podem ler, escrever e armazenar uma quantidade significativa de dados, assim como podem ser conectadas a sensores para armazenar e transmitir dados para e a partir desses dispositivos (NAEC et al., 2006).

Os preços das etiquetas ativas são bastante elevados em comparação com as etiquetas passivas, variando conforme a quantidade de memória, a vida útil da bateria, a presença de sensores e a robustez necessária. Um invólucro mais durável também aumenta o custo.

Etiquetas semi-passivas

Conforme Pedro (2008), etiquetas semi-passivas são um híbrido entre os dois tipos citados anteriormente, ativas e passivas. Esses tipos de etiquetas possuem uma fonte de energia interna (bateria) utilizada para alimentar o *microchip*. Entretanto ainda aproveitam a energia do campo eletromagnético com o leitor para se ativarem e iniciarem a transmissão de dados. Possuem um custo menor que as etiquetas ativas e um alcance maior que as passivas.

Etiquetas semi-passivas são utilizadas na coleta de pagamento de pedágio, controle de ponto de verificação e outros sistemas. Quando um carro se aproxima de uma praça de pedágio, o leitor envia um sinal que aciona o *transponder*. Este então emite uma onda de radiofrequência com o seu identificador para o leitor. Este tipo de etiqueta preserva a vida útil da bateria,

pois somente emite sinal quando está na zona de leitura do leitor (NAEC et al., 2006).



FIGURA 2.5 - Exemplos de etiquetas semi-passivas e ativas.

Fonte: GOMES, 2007, p.12.

Segundo Gomes (2007), considerando o tipo de memória empregada na etiqueta, é possível efetuar uma nova divisão dentro dos grupos supracitados:

- Somente leitura (*Read only*): permite somente a leitura dos dados gravados em memória. São programadas em fábrica uma única vez, as informações gravadas não podem ser atualizadas. Logo, riscos de adulteração são reduzidos. Etiquetas com esses tipos de memórias são empregadas geralmente em aplicações de pequeno porte, sendo inviáveis em grandes processos de manufatura. Etiquetas passivas são geralmente desse tipo.
- Única escrita e muitas leituras (*Write Once Read Many*): podem ser programadas, através de material indicado para esse fim, somente uma vez no momento adequado. Entretanto, na prática são gravadas mais vezes. Porém, deve-se evitar esse procedimento, pois um alto número de reprogramações pode danificar a memória.
- Leitura e Escrita (*Read Write*): geralmente podem ser reprogramadas entre 10.000 e 100.000 vezes, sendo que existem modelos com limites superiores. Esse tipo de

etiquetas normalmente possui uma memória Flash ou RAM. São mais caras que as demais, todavia apresentam facilidades como a possibilidade de atualização frequente dos dados e monitoração em tempo real de variáveis físicas.

Na Tabela 2.1 é apresentada uma comparação entre as etiquetas ativas e passivas.

TABELA 2.1 - Comparação entre etiquetas ativas e passivas.

Características	Passivas	Ativas
Bateria	Não	Sim
Fonte alimentação	Obtida do leitor	Interna
Vida útil	Longa	Limitada pela bateria
Manutenção	Desnecessária	Indispensável
Sinal leitor/etiqueta	Forte/Fraco	Fraco/Forte
Tamanho	Pequeno	Grande
Custo fabricação	Baixo	Elevado
Alcance de leitura	Curto (até 3 metros)	Longo (no mínimo 100 metros)
Memória	Pequena (na ordem de bytes)	Alta (na ordem de kB)
Capacidade de sensoramento	Capacidade de ler e transferir valores obtidos por sensores somente quando a etiqueta é alimentada pelo leitor; sem data/hora	Habilidade de continuamente monitorar e armazenar dados de sensores; data/hora para eventos dos sensores

Fonte: GOMES, 2007, p. 14.

2.2.2 Leitores

Uma aplicação de software desenvolvida para ler ou escrever dados em etiquetas RFID requer um leitor RFID como

interface. Do ponto de vista da aplicação. A transferência de dados não deve diferir das mesmas operações executadas em sistemas não-RFID (com contato). As operações de leitura e escrita são executadas tendo como base o princípio mestre-escravo, conforme a Figura 2.6. Isto significa que todas as atividades do leitor e das etiquetas são iniciadas pela aplicação de software. Em um sistema de estrutura hierárquica, a aplicação de software representa o mestre. Ao passo que o leitor representa o escravo, sendo ativado somente quando comandos de leitura/escrita são recebidos pela aplicação. Para executar um comando da aplicação de software, o leitor primeiro inicia a comunicação com a etiqueta, assumindo então o papel de mestre em relação a esta. As principais funções dos leitores são ativar a etiqueta, estruturar a sequência de comunicação e transferir dados entre a aplicação de software e a etiqueta. Todos os recursos da comunicação RFID são tratados pelo leitor (FINKENZELLER, 2010).

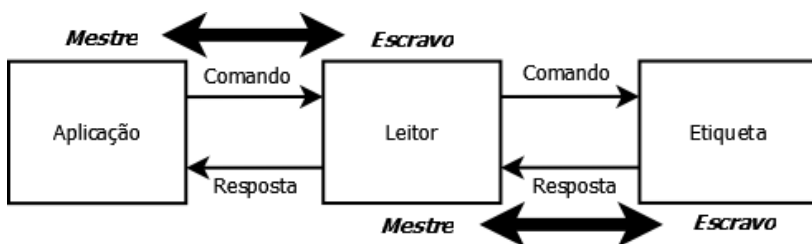


FIGURA 2.6 - Fluxo de dados entre aplicação, leitor e etiqueta.

Fonte: FINKENZELLER, 2010, p. 318.

Conforme Finkenzeller (2010), leitores em todos os sistemas podem ser reduzidos a dois blocos funcionais fundamentais: sistema de controle e interface de radiofrequência. Essa consiste de um transmissor e um receptor. A interface de RF executa as seguintes funções: geração de energia para transmissão em alta frequência para ativar a etiqueta e alimentá-la; modulação do sinal de transmissão para enviar dados à etiqueta; recepção e demodulação do sinal RF transmitido pela

etiqueta. No projeto de um leitor deve haver a preocupação em proteger esse módulo contra emissões indesejadas. A unidade de controle é responsável por: comunicação com a aplicação de software e execução dos comandos encaminhados por esta; controle de comunicação com a etiqueta (princípio mestre-escravo); codificação e decodificação do sinal. Em sistemas mais complexos estão disponíveis funções adicionais, como: execução de algoritmo anti-colisão; criptografia e descryptografia de dados transferidos entre leitor e etiqueta; execução de autenticação entre leitor e etiqueta. Na Figura 2.7 são representados os blocos fundamentais de um leitor.

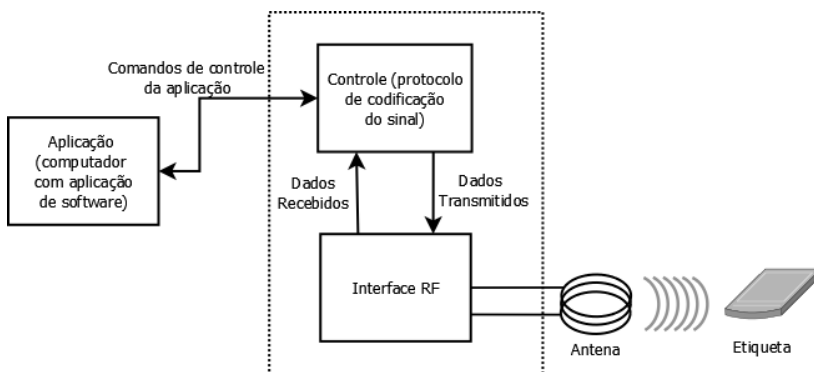


FIGURA 2.7 - Componentes principais do leitor.

Fonte: FINKENZELLER, 2010, p. 319.

A unidade de controle utiliza um microprocessador para executar estas funções complexas. Procedimentos de criptografia, assim como cifragem do conjunto de dados e codificação são executados em um módulo ASIC adicional para liberar o processador de cálculos complexos. (FINKENZELLER, 2010).

Conforme Almeida (2011), normalmente os leitores possuem somente uma antena interna, mas existem modelos que podem controlar várias antenas distantes entre si. Também é

possível configurar uma antena somente para transmissão e outra para recepção. O modelo de antena deve ser considerado na implantação de sistemas RFID, pois influencia diretamente na área de cobertura, alcance e acurácia da comunicação. Determinados modelos podem apresentar bom alcance, mas em contrapartida não apresentam bons resultados quando há variações na orientação da antena do leitor com a da etiqueta. O *layout* dos leitores varia em formato, tamanho e manuseio, logo também deve ser considerado no momento da implantação.

Leitores também podem disponibilizar canais de entrada e saída para uso de anunciadores², atuadores e sensores externos. Os leitores não leem etiquetas constantemente, logo deixá-los ativos em tempo integral seria um desperdício de energia. Visando melhorar o rendimento dos leitores, são adotados sensores de movimento ou de luz que ativam o leitor somente quando um objeto entra na zona de leitura. Similarmente, pode-se também utilizar um anunciador para gerar um alarme sonoro ou um atuador para abrir ou fechar automaticamente uma porta, por exemplo (LAHIRI, 2005).

Lahiri (2005) ressalta que leitores RFID podem ser classificados usando dois critérios diferentes. O primeiro critério é a interface disponibilizada para comunicação com a aplicação do sistema. Baseados neste, leitores são divididos em:

- **Seriais:** estes tipos precisam de um *link* de comunicação serial para se comunicarem com a aplicação. Os leitores são fisicamente conectados à porta serial do computador utilizando a interface RS232 ou RS485. A vantagem desses leitores quando comparados com os leitores de rede é que são mais confiáveis. Porém, possuem desvantagens como a limitação da conexão pelo tamanho do cabo, o número de interfaces seriais disponíveis no computador limita a quantidade de leitores que podem ser conectados, e a taxa de transmissão é mais baixa que em uma rede de dados.

² Conforme Lahiri (2005), anunciadores atuam como indicadores, por exemplo, alarmes sonoros e luzes.

- De rede: podem ser conectados a um computador através de redes com fio e sem fio. O leitor comporta-se como um dispositivo de rede qualquer que dispensa conhecimento de hardware. Alguns modelos de leitores permitem inclusive monitoração SNMP (*Simple Network Management Protocol*). A atualização do firmware pode ser realizada remotamente via rede, agilizando e reduzindo os custos dos processos de manutenção. Uma desvantagem desses leitores é que quando se perde conexão com a rede o leitor fica incomunicável, podendo provocar a paralisação do sistema RFID. A fim de reduzir esse transtorno, alguns leitores possuem uma memória interna para armazenar informações sobre as etiquetas lidas.

O segundo critério de classificação apresentado por Lahiri (2005) é a mobilidade, que divide os leitores em:

- Fixos: são os tipos mais comuns, podem ser montados sobre uma parede, em um portal ou alguma estrutura adequada dentro da zona de leitura. Essas estruturas podem ser, por exemplo, empilhadeiras e caminhões de entrega. Leitores fixos geralmente necessitam de antenas externas e possuem custo menor em relação aos portáteis. Geralmente, operam em dois modos: autônomo e interativo. No modo autônomo, o leitor efetua a leitura das etiquetas continuamente e armazena as informações em uma lista, que é enviada periodicamente para a aplicação. No modo interativo, o leitor recebe e executa comandos da aplicação. Quando finaliza um comando, ele aguarda pelo próximo.
- Portáteis: podem ser utilizados como unidades portáteis e geralmente possuem antenas internas. Embora esses leitores sejam mais caros, o avanço da tecnologia tem proporcionado leitores mais sofisticados e preços menores.

2.3 Termos técnicos

Lahiri (2005), lista alguns termos que são frequentemente utilizados em discussões relacionadas a sistemas RFID e que são importantes para a compreensão do seu funcionamento:

- Colisão de etiquetas: um leitor somente pode se comunicar com uma etiqueta por vez. Quando mais de uma etiqueta tenta comunicar-se com um mesmo leitor ao mesmo tempo, ocorre uma colisão de etiquetas, ou seja, múltiplas etiquetas refletem seus sinais para o leitor, confundindo-o. Para contornar esse problema, são empregados algoritmos de anti-colisão que permitem ao leitor identificar diversas etiquetas em sua zona de leitura em um curto período de tempo.
- Colisão de leitores: quando a zona de leitura de dois ou mais leitores se sobrepõe, pode haver interferência no sinal, pois a energia da antena de um dos leitores pode anular a energia do outro, caracterizando uma colisão de leitores. Para evitar esse problema, pode-se mudar a posição das antenas, separar os leitores (eliminando a sobreposição das zonas de leitura) ou empregar TDMA (*Time Division Multiple Access*). Nesse caso, os leitores são configurados para lerem em intervalos distintos. Consequentemente, somente um leitor estará ativo por vez.
- Legibilidade de etiquetas: é definida como a capacidade de um sistema ler dados de uma determinada etiqueta com sucesso. A fim de garantir o sucesso na leitura, o sistema deve ser projetado para ler a mesma etiqueta diversas vezes, pois mesmo que ocorram falhas há grandes chances de ao menos uma leitura ser bem sucedida.
- Robustez na leitura: também conhecido como redundância, é a quantidade de vezes que uma determinada etiqueta

pode ser lida com sucesso quando dentro da zona de leitura. A velocidade de um objeto etiquetado pode impactar negativamente na robustez, pois quanto mais rápido o deslocamento do objeto, menor o tempo que estará dentro da zona de leitura. A quantidade de etiquetas presentes simultaneamente na mesma zona também reduz a robustez, visto que o número de etiquetas que podem ser lidas por um leitor em um determinado intervalo de tempo é limitado.

2.4 Frequência de operação

Devido ao fato de sistemas RFID gerarem e irradiarem ondas eletromagnéticas, eles são classificados como sistemas de rádio. O funcionamento de outros dispositivos de rádio não deve ser, em circunstância alguma, interrompido ou prejudicado pela operação de sistemas RFID, ou seja, não devem interferir em: rádio, televisão, rádio móvel (polícia, segurança, indústria), serviços de rádio da marinha/aeronáutica e telefones celulares (FINKENZELLER, 2010).

Segundo Hodges e Harrison (2003), devido à importância da comunicação, o espectro eletromagnético é controlado por governos em todo o mundo. Algumas frequências de transmissão de ondas eletromagnéticas têm efeito muito limitado. A luz visível, por exemplo, pode ser facilmente atenuada ou bloqueada. Entretanto, ondas de rádio são consideradas mais difusivas, um transmissor em um edifício/cidade/país pode impactar significativamente em um receptor localizado em outro edifício/cidade/país. A fim de evitar problemas como esse, as transmissões de ondas de rádio são controladas por tratados nacionais e internacionais, que especificam amplitudes, frequências, mecanismos de comunicação e aplicações permitidas nos sistemas através de um processo conhecido como licenciamento do espectro. Porém, como inicialmente os governos de cada país eram responsáveis pelo licenciamento do

espectro em sua localidade, atualmente diferentes países possuem diferentes alocações de frequências.

A maioria dos sistemas RFID operam na banda ISM (*Industrial, Scientific and Medical*) definida pelo ITU-T (*International Telecommunication Union - Telecommunication Standardization Sector*), a qual não exige licenciamento da estação, pois a baixa potência utilizada não provoca interferências (FINKENZELLER, 2010).

As faixas de frequências utilizadas em sistemas RFID podem ser agrupadas em quatro grupos: baixas, altas, ultra altas e microondas. Sistemas RFID que operam em baixas frequências (125 kHz-134 kHz), geralmente utilizam etiquetas passivas, tem faixa de operação aceita mundialmente, apresentam baixas taxas de transferências e se comportam muito bem em ambientes com líquidos ou sujeiras. Os sistemas em baixas frequências são os mais antigos, logo há uma grande quantidade em operação. Sistemas que operam em altas frequências (13,56 MHz) normalmente utilizam etiquetas passivas, têm baixa taxa de transferência e bom desempenho na presença de metais e líquidos. Além disso, sua faixa é aceita mundialmente e são amplamente utilizados em hospitais por não interferirem nos equipamentos existentes. Sistemas que operam em frequências ultra altas não possuem um consenso global. Dividem-se em sistemas passivos que operam com 915 MHz nos Estados Unidos e 868 MHz na Europa, já sistemas ativos utilizam as frequências de 315 MHz e 433 MHz. Sistemas que operam na faixa de micro-ondas utilizam 2,45 GHz ou 5,8 GHz, sendo a primeira mais comum, podem utilizar etiquetas passivas e semi-passivas, apresentam altas taxas de transferências, e baixo desempenho em ambientes com líquidos e metais (LAHIRI, 2005).

A Tabela 2.2 apresenta um comparativo entre essas faixas considerando as principais características que devem ser avaliadas no planejamento de uma solução RFID.

TABELA 2.2 - Comparativo entre frequências RFID.

Frequências	Baixas 125-134 kHz	Altas 13,56 MHz	Ultra altas ~300-1000MHz	Microondas 2,4-5,8 GHz
Disponibilidade	>30 anos	>10 anos	Recente	>10 anos
Padronização	ISO 11784/5, ISO14223, ISO18000-2	ISO 14443 , ISO 15693, ISO18000-3	ISO 18000-6, EPCGen1and2	ISO18000-4
Líquidos	Sem impacto	Baixo impacto	Alto impacto	Alto impacto
Leitura múltipla	Limitado	Acima de 50 etiquetas/segundo	Acima de 150 etiquetas/segundo	Indefinido
Alcance leitura	Até 100 cm	Até 50 cm	EUA - Até 500 cm Europa - Até 300 cm	Até 500 metros, etiquetas ativas
Taxa de transferência de dados	Lenta	Média	Rápida	Muito rápida
Resistência à interferência	Alta	Alta	Depende do ambiente	Suscetível a ruído eletrônico
Aplicações típicas	Identificação animal, controle de acesso, identificação pessoal	Controle de alimentos, identificação de itens, controle de acesso	Gestão da cadeia de suprimentos, rastreamento de <i>contêineres</i>	Sistemas de localização em tempo real, controle de acesso de veículos de longo alcance

Fonte: NAEC et al., 2006, p. 14.

Conforme Hodges e Harrison (2003), em muitos locais é possível solicitar aos órgãos reguladores do espectro de rádio permissão especial para utilizar equipamentos operando fora da legislação em vigor. Isso pode ser útil no desenvolvimento de novos equipamentos RFID ou na utilização temporária de um sistema RFID não compatível, sendo que fatores como localização e potencial de interferência serão avaliados.

2.5 Padronização

A indústria RFID tem sido impulsionada por aplicações em diversas áreas. Vislumbrando essas oportunidades, diferentes fornecedores de tecnologia para desenvolvimento de produtos RFID se preocuparam em suprir as necessidades do mercado, mas não consideraram a compatibilização de seus produtos com os de outros fornecedores. Essa falta de padronização é considerada uma barreira para uma aprovação mais ampla da tecnologia. Muitas aplicações exigem a interoperabilidade entre produtos de diferentes fornecedores e/ou de sistemas em diferentes regiões. A fim de reduzir esses problemas, foram criadas várias especificações com o objetivo de padronizar aspectos da operação de sistemas RFID (HODGES E HARRISON, 2003).

Conforme Junior (2010), o processo de elaboração de padrões ainda está em desenvolvimento, entretanto eles tendem a cobrir basicamente quatro áreas chaves dentro das aplicações RFID: interfaces de ar (comunicação entre leitores e etiquetas), conteúdo e codificação de dados, testes de conformidade com as normas e interoperabilidade entre sistemas.

A seguir são apresentadas as principais organizações reguladoras para sistemas RFID:

- EAN.UCC: a associação EAN (*European Article Number Association*) e a UCC (*Universal Code Council*), são responsáveis pela co-gestão do sistema EAN.UCC e GSMP (*Global Standard Management Process*). O sistema EAN.UCC mantém e estabelece normas para códigos de barra, conjunto de transações EDI (*Electronic Data Interchange*), esquemas XML e outras soluções da cadeia de suprimentos. Ao administrar a distribuição de prefixos para companhias e coordenar as normas explicativas, a EAN e a UCC tendem a tornar os sistemas de identificação de itens mais robustos em todo o mundo. O EAN.UCC também é responsável pela especificação das funções de

monitoramento/rastreamento e sincronização de dados (SWEENEY II, 2005).

- EPCGlobal: fundada em 2003 pela EAN e UCC, atualmente lidera o desenvolvimento de normas impulsionadas pela indústria relacionadas ao EPC³ (*Electronic Product Code*) para suporte ao uso de identificação por radiofrequência. A EPCGlobal é responsável pela atribuição de blocos de números para seus membros, e também tem definido o protocolo EPC para etiquetas, que compreende a estrutura de dados escritas na etiqueta e o protocolo da interface de ar. Ela também tem trabalhado no desenvolvimento de uma tecnologia de transferência de dados, denominada EPCglobal Network. Essa tecnologia permite a parceiros comerciais documentar e localizar bens individuais e mercadorias na cadeia de suprimentos em tempo real. Informações adicionais como data de validade podem ser transferidas facilmente. Os objetos são registrados com leitores RFID que são conectados via interface de software a serviços na Internet disponíveis pela EPCglobal. A combinação da aquisição de dados via RFID com o fornecimento, distribuição e conexão desses dados via internet oferece um grande potencial para melhorar os processos logísticos nos comércios nacionais e internacionais (SWEENEY II, 2005) (FINKENZELLER, 2010).
- UCCnet: trata-se de uma subsidiária da UCC, é uma organização sem fins lucrativos que fornece uma base eletrônica para aplicação de normas desenvolvidas para a indústria. A UCCnet armazena um catálogo de dados relacionados a itens e fornece um mecanismo de sincronização de dados entre empresas que utilizam a plataforma UCCnet. Enquanto a EPCGlobal mantém um

³ EPC disponível somente na faixa de frequências ultras altas, é a próxima geração de identificação de produtos. Divide-se em números que podem identificar o fabricante e o tipo de produto, utiliza um número de série que permite identificar itens exclusivos em movimento na cadeia de suprimentos (NAEC et al., 2006).

registro dos números dos produtos, a UCCnet mantém os detalhes associados a esses dados. Exemplificando, um fornecedor irá associar os detalhes de um produto a um número EPC e encaminhará para a UCCnet essas informações. O varejista, que irá receber esse produto, atualizará sua base com as informações da UCCnet e terá conhecimento do número e especificação do produto recebido, facilitando o controle de estoque (SWEENEY II, 2005).

- ISO/IEC JT1: a ISO (*International Standards Organisation*) e a IEC (*International Electrotechnical Commission*) formaram um comitê, o JT1 (*Joint Technical Committee 1*), para estabelecer normas de sistemas RFID. Essas normas se aplicam a diferentes tipos de aplicações e a diferentes frequências de operação. Para sistemas de identificação operando a altas frequências são utilizadas as normas ISO 10536, ISO 14443 e ISO 15693. A norma ISO 18000 se divide em sete partes que descrevem a comunicação da interface de ar em diferentes frequências. (MONTEIRO, PACHECO E LIMA, 2003).
- AIAG (*Automotive Industry Action Group*): é uma organização profissional que trabalha com questões da cadeia de suprimentos do setor automobilístico. Sua missão é propor normas industriais e fornecer orientações para a indústria automobilística. O padrão de dados que a AIAG definiu para pneus é chamado de B-11. Ele disponibiliza informações sobre o fabricante, tamanho e tipo dos pneus, além de outras informações adicionais (SWEENEY II, 2005).

No Brasil, a ANATEL (Agência Nacional de Telecomunicações) é responsável por determinar como equipamentos de radiofrequência podem utilizar o espectro para a transmissão de sinais. A Resolução número 506, de 1 de julho de 2008, “*Regulamento Sobre Equipamentos de Radiocomunicação de Radiação Restrita*”, determina que equipamentos de radiação restrita, onde se enquadram leitores RFID, são dispensados de cadastramento para instalação e

operação, mas precisam passar por processos de homologação, assim como etiquetas ativas.

3. MODELO PARA CONTROLE DE ACESSO EM ESTACIONAMENTOS

O sistema elaborado neste projeto emprega a tecnologia de identificação por radiofrequência aplicada em um sistema embarcado. Neste capítulo é apresentada a descrição completa do modelo proposto, sendo que, primeiro, descreve-se o funcionamento básico do sistema e, em seguida, é feita a especificação do hardware escolhido para elaboração de um protótipo.

3.1. Definição

Sistemas com tecnologia RFID podem ser classificados em três tipos: autônomos, aqueles que não são interligados a outros sistemas; *loop* fechado, que restringem-se a uma única organização; e *loop* aberto, que envolvem múltiplos parceiros, como em uma cadeia de varejo e seus fornecedores (OECD, 2008). Neste trabalho optou-se pelo desenvolvimento de um sistema autônomo, devido à reduzida complexidade na implementação quando comparado aos demais.

O modelo proposto foi elaborado com o objetivo de efetuar controle de acesso através de etiquetas RFID e permitir ao administrador do sistema visualizar os registros de acesso. A infraestrutura desenvolvida divide-se basicamente em dois módulos: aplicação web, responsável pela apresentação dos registros de entrada/saída, e o sistema microcontrolado, que tem como principal função realizar o controle de acesso. Esses dois módulos são detalhados nos tópicos a seguir.

A tecnologia de radiofrequência na identificação dos usuários foi escolhida devido a sua praticidade. A RFID possibilita a transferência de dados mesmo sem necessidade de contato físico, a leitura é realizada de forma rápida e as etiquetas são resistentes ao longo do tempo, mantendo-se funcionais

ainda que expostas a ambientes inadequados, como por exemplo, com umidade e sujeira. Em relação às etiquetas, foram preferidas as passivas fabricadas para baixas frequências, devido aos seguintes fatores:

- O alcance para leitura não precisa ser longo, visto que o veículo poderá se posicionar próximo ao leitor.
- O custo dessas etiquetas é inferior ao das demais.
- Reaproveitamento de etiquetas utilizadas em sistemas de ponto eletrônico.

Inicialmente não se identificou a necessidade de alterar os dados das etiquetas, logo não serão adotados leitores com possibilidade de escrita, somente de leitura.

Não é objetivo deste projeto implementar um cenário real. Pretende-se apenas montar um protótipo que valide as funções de controle de acesso, gerenciamento da quantidade de vagas e armazenamento de dados. Logo, para simular o painel com a informação sobre a quantidade de vagas será utilizado um *display* LCD (*Liquid Crystal Display*) alfanumérico 20 x 4 (vinte caracteres por linha, com quatro linhas) e para representar a abertura dos portões serão utilizados servomotores.

Na Figura 3.1 é apresentado de forma simplificada o modelo proposto. O número identificador obtido pelo leitor RFID é enviado para o microcontrolador, que após realizar o devido processamento envia para o servidor web o registro de entrada ou saída. O servidor web é composto por um banco de dados e uma aplicação web, sendo que no banco ficam armazenados os registros de acesso e as informações sobre funcionários e veículos, ao passo que a aplicação é utilizada pelo usuário para a consulta e o cadastro de informações.

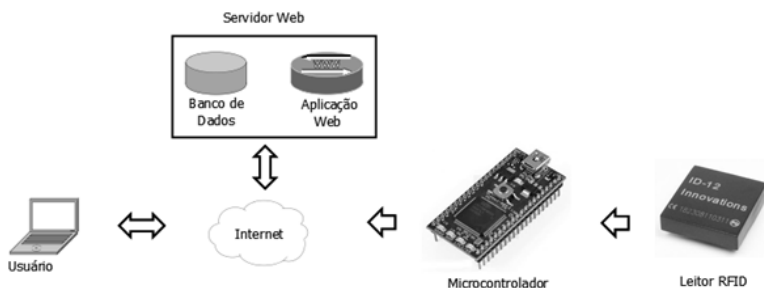


FIGURA 3.1 - Modelo do sistema de controle de acesso.

3.2. Sistema microcontrolado

O módulo de controle de acesso tem como núcleo o microcontrolador, responsável por contabilizar as vagas disponíveis, apresentar essa informação via *display*, acionar as cancelas, autorizar o acesso aos usuários via conferência do identificador fornecido por um leitor RFID e alimentar a base de dados com os registros de acesso.

Conforme a Figura 3.2, o sistema dispõe de dois leitores RFID, um dedicado para a entrada de veículos e outro para a saída, sendo que ambos serão controlados pelo mesmo microcontrolador. No portão de entrada, há um *display* para informar a quantidade de vagas disponíveis, evitando filas em casos de lotação máxima, por exemplo. Sempre que um usuário entra no estacionamento, a quantidade total de vagas é subtraída de uma unidade, ocorrendo o inverso na saída.

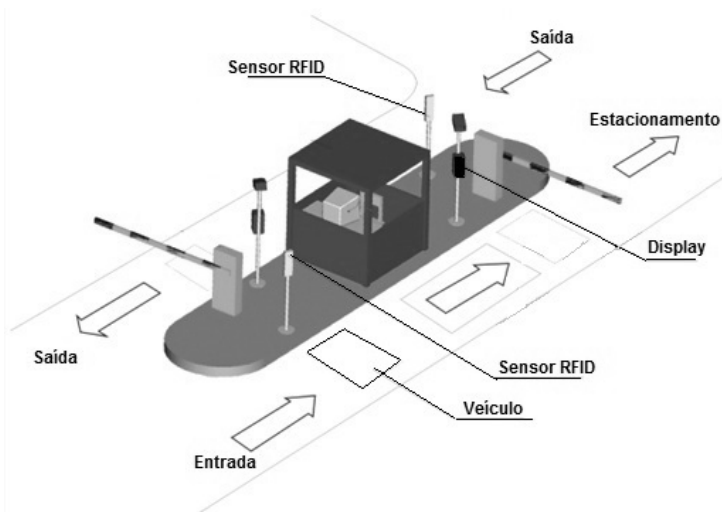


FIGURA 3.2 - Estacionamento com controle de acesso.

Fonte: GAO RFID Inc, 2013.

O sistema de controle armazena em arquivo uma lista com os códigos de identificação das etiquetas que possuem acesso liberado. Esse identificador é informado pelo leitor RFID e o microcontrolador verifica se ele está na sua lista de IDs (identificadores) autorizados. Conforme os registros de acesso são realizados, eles são enviados pelo microcontrolador para o banco de dados via rede de dados. O microcontrolador também mantém um arquivo que armazena a quantidade de vagas disponíveis. Na configuração inicial do sistema esse arquivo deve ser configurado com a quantidade máxima de vagas do estacionamento, sendo que esse deve estar vazio.

A tecnologia RFID está em um estágio de desenvolvimento no qual a privacidade e a segurança são identificadas como desafios para sua adoção. Com o intuito de garantir privacidade e segurança, os sistemas devem apresentar disponibilidade (garantia de acesso a informações ou recursos quando necessário), integridade (segurança de que os dados não serão alterados durante a transmissão) e confidencialidade

(informação deve estar disponível somente para usuários autorizados) (OECD, 2008). Porém, no modelo proposto não está sendo considerada a possibilidade de ataques ao sistema devido a grande complexidade em atender a todos os critérios necessários para garantir disponibilidade, integridade e confidencialidade. Todavia, garante-se um certo grau de disponibilidade ao modelo, pois optou-se por armazenar a lista de identificadores com permissão de acesso em um cartão de memória, acessível ao microcontrolador, garantindo que o sistema irá continuar operando mesmo em caso de perda de conexão com a rede de dados. Entretanto, não é previsto o armazenamento local dos registros de acesso realizados no período em que a rede estiver fora de alcance, logo essas informações não serão disponibilizadas ao usuário.

Na Figura 3.3 é apresentado o fluxograma do processo de inicialização do sistema microcontrolado. Primeiramente é inicializada a rede de dados através da associação de um IP a placa de rede. Em seguida são configurados os servomotores e ajustados para a posição inicial, cancelas fechadas. Após, a lista com os identificadores é carregada em um vetor e a quantidade de vagas disponíveis é lida de um arquivo e armazenada em uma variável. Se não houver vagas disponíveis o display informa lotação máxima, caso contrário é apresentado no display a quantidade de vagas disponíveis. Posteriormente os leitores RFID são inicializados e o microcontrolador entra em um laço infinito no qual é realizada a monitoração do leitor RFID de entrada, se o microcontrolador recebe o identificador ele executa o fluxograma do procedimento de entrada, caso contrário ele monitora o leitor RFID de saída, se o microcontrolador receber o identificador ele executa o fluxograma do procedimento de saída, caso contrário volta a monitorar o leitor de entrada e assim sucessivamente.

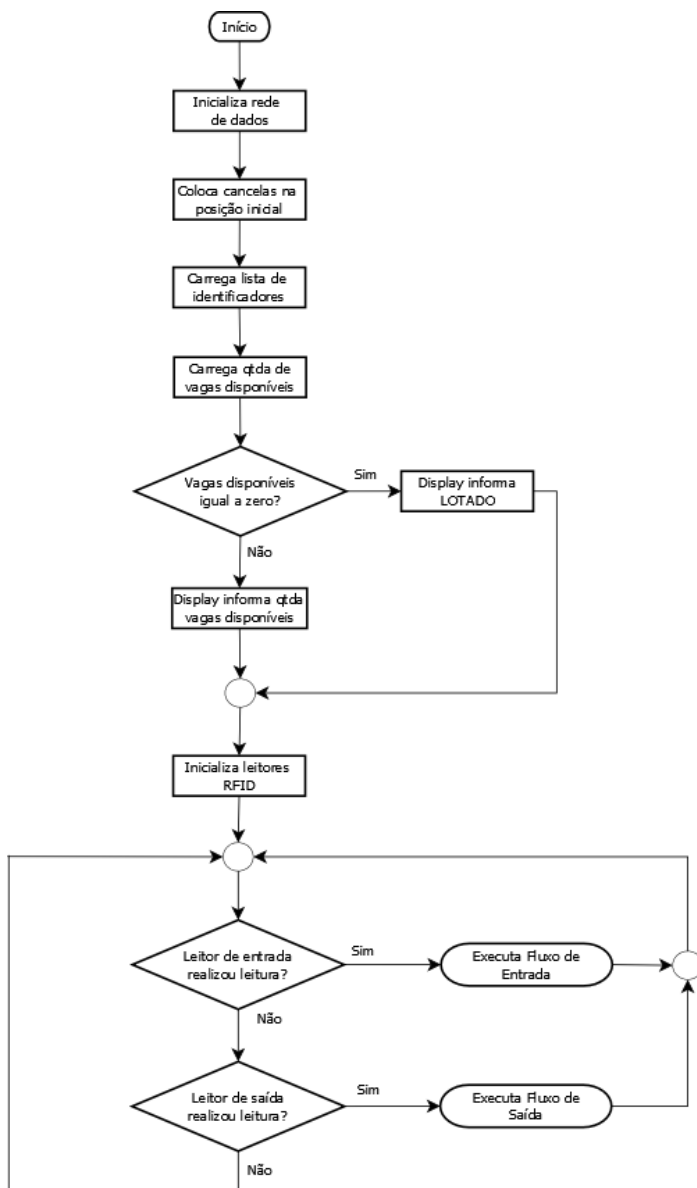


FIGURA 3.3 – Fluxograma do procedimento de inicialização do sistema microcontrolado.

Na Figura 3.4 é apresentado o fluxograma do processo a ser seguido pelo sistema quando o usuário efetuar uma tentativa de acesso. Assim que a etiqueta aproxima-se do leitor RFID, o código de identificação é enviado ao microcontrolador. Este verifica se a informação recebida consta na lista de identificadores. Caso a identificação não seja encontrada, o servomotor não é acionado e por alguns segundos o *display* informa que o identificador não possui autorização de acesso. Após finalizar o tempo configurado, o *display* volta a apresentar a quantidade de vagas disponíveis ou a informação de lotação máxima.

Quando a identificação consta na lista de identificadores, é verificado se há vagas disponíveis. Caso todas as vagas estejam ocupadas, o *display* estará mostrando a informação de lotação máxima, o servomotor não é acionado e um registro de falha na tentativa de acesso devido à lotação é inserido no banco de dados. Entretanto, se houver vagas disponíveis, o acesso é liberado. Logo, a quantidade de vagas livres é decrementada e atualizada em arquivo, o *display* informa a quantidade de vagas livres (ou lotação máxima, se for o caso), o servomotor é acionado, representando a abertura do portão e um registro de acesso é inserido no banco de dados. Sempre que houver alterações na quantidade de vagas, esse valor é atualizado em um arquivo, a fim de evitar que a informação fique inconsistente, como no caso de o sistema reiniciar.

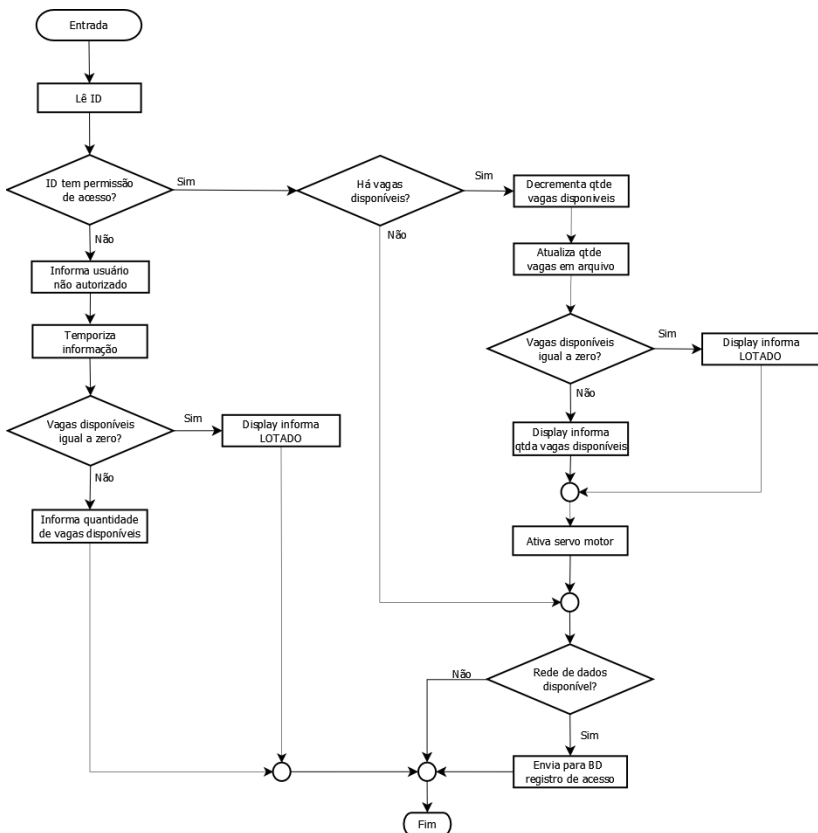


FIGURA 3.4 - Fluxograma do procedimento de entrada.

O procedimento executado na saída dos veículos é bastante simples. Inicialmente é verificado se o identificador possui permissão de saída, caso negativo nenhuma ação é adotada. Se o identificador possuir permissão de saída o número de vagas disponíveis é incrementado, o servomotor é acionado e é realizada a inserção de um registro de saída no banco de dados. Na Figura 3.5 é apresentado o fluxograma do processo a ser executado pelo sistema na saída de um veículo. O incremento da quantidade de vagas disponíveis é limitado pela capacidade máxima do estacionamento.

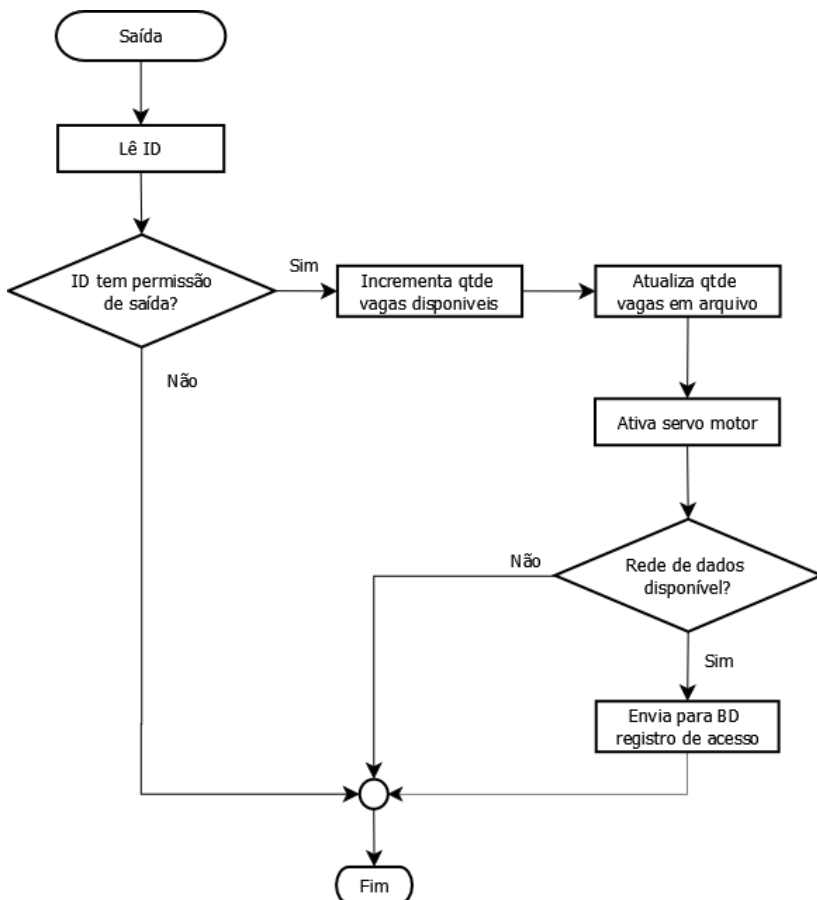


FIGURA 3.5 - Fluxograma do procedimento de saída.

3.3. Aplicação Web

O módulo de apresentação de registros consiste em uma aplicação web que possibilita ao usuário realizar inclusão, exclusão e consulta de funcionários e veículos, assim como

consultar os registros de acesso por período. Todas as informações são armazenadas em um banco de dados que é acessado pela aplicação.

Foi dada preferência à adoção de uma aplicação web para garantir flexibilidade e praticidade, pois o acesso pelo usuário não estará limitado a computadores específicos, o que ocorre quando emprega-se soluções *stand-alone*. Além disso, a manutenção se torna mais fácil, visto que a atualização da aplicação é feita somente no servidor e possibilita maior independência do sistema operacional. Outros fatores que reforçam a escolha da aplicação web são: não ocupa espaço local no computador dos usuários, é necessário apenas um *browser* para poder acessar a aplicação (dispensando instalação de softwares adicionais).

A adoção de um sistema web implica em ficar vulnerável a problemas relacionados com a conexão à rede de dados, porém isso afeta somente as operações de consulta e cadastro. O controle de acesso permanece funcionando mesmo se ocorrerem falhas no acesso a rede de dados.

3.4. Especificação dos dispositivos utilizados

Microcontrolador

Considerando-se que o tempo para o desenvolvimento do projeto foi limitado, optou-se por uma placa de desenvolvimento microcontrolada, proporcionando maior agilidade e flexibilidade durante o processo de elaboração do protótipo. A placa escolhida foi a mbed, conforme Figura 3.6. A mbed fornece todos os periféricos necessários para a implementação do modelo proposto neste trabalho, como saídas digitais, PWM (*Pulse-Width Modulation*), interfaces de comunicação serial e SPI (*Serial port interface*).

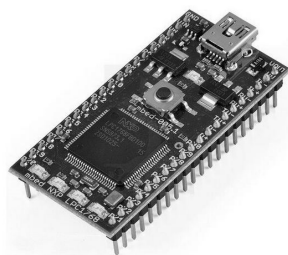


FIGURA 3.6 - Placa de desenvolvimento ARM mbed NXP LPC1768.

Fonte: Mbed, 2013.

A plataforma mbed tem origem com o trabalho de dois funcionários da ARM, que pretendiam elaborar um ambiente de desenvolvimento rápido. Mais tarde, a ARM, em parceria com a NXP *Semiconductors*, assumiu o projeto. Um ponto forte dessa plataforma é a biblioteca mbed, que fornece uma abordagem para codificação orientada a API (*Application Programming Interface*), eliminando grande parte do trabalho de baixo nível, normalmente associado com o desenvolvimento de código para o microcontrolador. O código pode ser desenvolvido usando abstrações e chamadas a APIs, possibilitando ao desenvolvedor focar nas regras de negócio, sem se preocupar com a implementação do núcleo do microcontrolador ou de seus periféricos (Mbed, 2013).

O ambiente de desenvolvimento é baseado em computação na nuvem (*cloud computing*), não havendo necessidade da instalação de ferramentas para programação e compilação. Todo o processo é efetuado através de um *browser*, tornando-o independente do sistema operacional. O ambiente também disponibiliza um sistema de controle de versão para que o usuário possa gerenciar diferentes versões do seu projeto. Após a compilação, a gravação do *firmware* é muito simples, ao conectar no computador a placa via USB (*Universal Serial Bus*), o *driver* MBED é automaticamente criado.

O projeto mbed disponibiliza espaço na nuvem para que os desenvolvedores compartilhem suas informações, bibliotecas, componentes e tutoriais.

A mbed é baseada no NXP LPC1768, um microcontrolador ARM (*Advanced Risc Machine*) Cortex-M3 rodando a 96 MHz. Possui memória *flash* de 512 kB, RAM (*Random Access Memory*) de 32 kB e vários periféricos, conforme Tabela 3.1. A montagem do microcontrolador e demais componentes na mbed é feita de tal forma que a placa resulta em formato semelhante ao encapsulamento duplo em linha (DIP - *Dual in-line package*) com 40 pinos, apresentando a facilidade de poder ser encaixada em qualquer matriz de contatos para suporte a montagem de protótipos. Pode ser alimentada via USB (5 V) ou através de fonte externa (4,5 V a 9 V).

TABELA 3.1 - Periféricos mbed NXP-1768.

Periférico	Quantidade
Ethernet	1
USB <i>Host</i>	1
USB <i>Device</i>	1
SPI	2
I2C (<i>Inter-Integrated circuit</i>)	2
CAN (<i>Controller-Area Network</i>)	2
Entradas analógicas	6
Saídas analógicas	1
Saída PWM	6
UART (<i>Universal Asynchronous Receiver/Transmitter</i>)	3

Leitor RFID

Para a leitura das etiquetas RFID, pesquisou-se um módulo que fosse compacto e de fácil utilização, por fim adotou-se o ID-12 da *ID Innovations*, ver Figura 3.7.



FIGURA 3.7 - ID-12 *Innovations*.

O modelo ID-12 possui antena interna e suporta formatos de dados em ASCII, *Wiegand26* e *Magnetic ABA (American Bankers Association) Track2*⁴. Suas demais características são apresentadas na Tabela 3.2.

⁴ *Magnetic ABA Track2*: formato de dados definido pela associação de banqueiros americanos para ser utilizado mundialmente em cartões de crédito magnéticos.

TABELA 3.2 - Características leitor RFID

Parâmetro	ID-12
Alcance de leitura	12 cm
Dimensões	26 mm x 25 mm x 7 mm
Frequência	125 kHz
Formato de dados	EM4001 ou compatível
Codificação	Manchester 64-bit
Alimentação	5 VDC (consumo de 30 mA)
Transferência de dados	RS232/9600 bps

Fonte: ID Innovations, 2005.

Para facilitar o manuseio do RFID durante os testes na *protoboard* e sua conexão na placa de circuito impresso, foi utilizada uma placa adaptadora, conforme a Figura 3.8, na qual o RFID foi conectado.

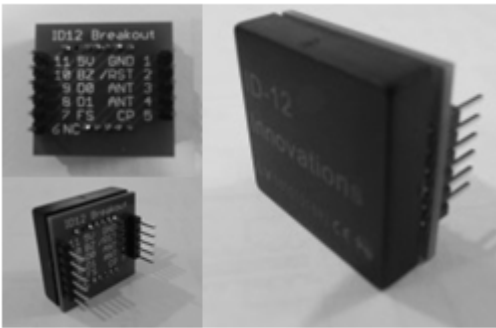


FIGURA 3.8 - Placa adaptadora do leitor RFID.

Etiquetas

As etiquetas foram escolhidas com base no leitor RFID, obedecendo aos critérios de compatibilidade.

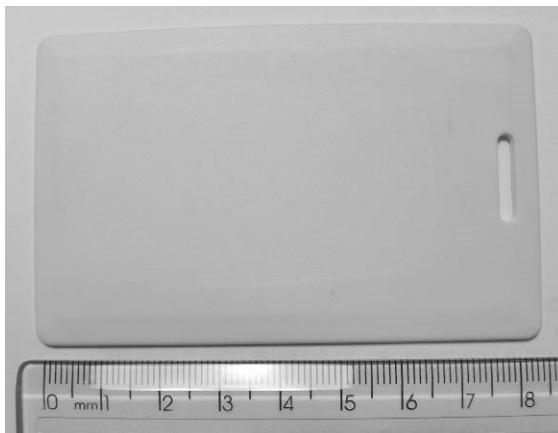


FIGURA 3.9 - Etiqueta RFID.

Optou-se por modelos não reprogramáveis, em formato de cartão, conforme Figura 3.9. Na Tabela 3.3 são apresentadas as características das etiquetas utilizadas.

TABELA 3.3 - Características da etiqueta RFID empregada.

Parâmetro	ID-12
Frequência	125 kHz
Dimensões	54 mm x 85,5 mm x 0,8 mm
Identificador	32 bits
Formato de dados	EM4001
Codificação	Manchester 64-bit

Fonte: SPARKFUN, 2013.

Cartão de memória

dispositivo escolhido possui velocidade de 0,10s/60 graus a 4,8 V, podendo ser alimentado de 3 a 6 V.

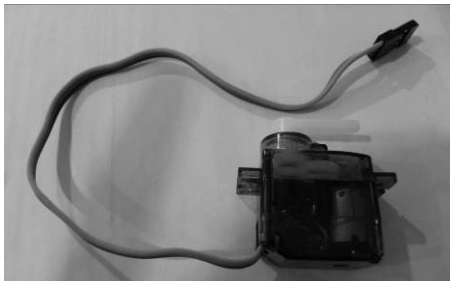


FIGURA 3.11 - Micro Servomotor.

Ethernet

Para possibilitar a comunicação do sistema com a internet, foi adotado um conector RJ45 10/100 Base-TX com transformador magnético integrado. Optou-se pelo modelo com transformador, pois ele atua como um filtro, logo possibilita conexão segura com modems ADSL, *switches* e *hubs*.

4. IMPLEMENTAÇÃO DA ARQUITETURA

Neste capítulo, são apresentadas as ferramentas empregadas e os detalhes de implementação aplicados no desenvolvimento e construção do protótipo.

4.1 Ferramentas utilizadas

O software embarcado foi implementado em linguagem de programação C. Como ambiente de desenvolvimento foi adotada a ferramenta mbed *Compiler*, que trata-se de uma IDE (*Integrated Development Environment*) online, mantida pelo projeto Mbed. Essa ferramenta utiliza o compilador ARMCC.

Na Figura 4.1 é apresentada a IDE utilizada na elaboração deste projeto. No lado esquerdo estão todos os projetos em desenvolvimento e no centro ficam os arquivos em edição.

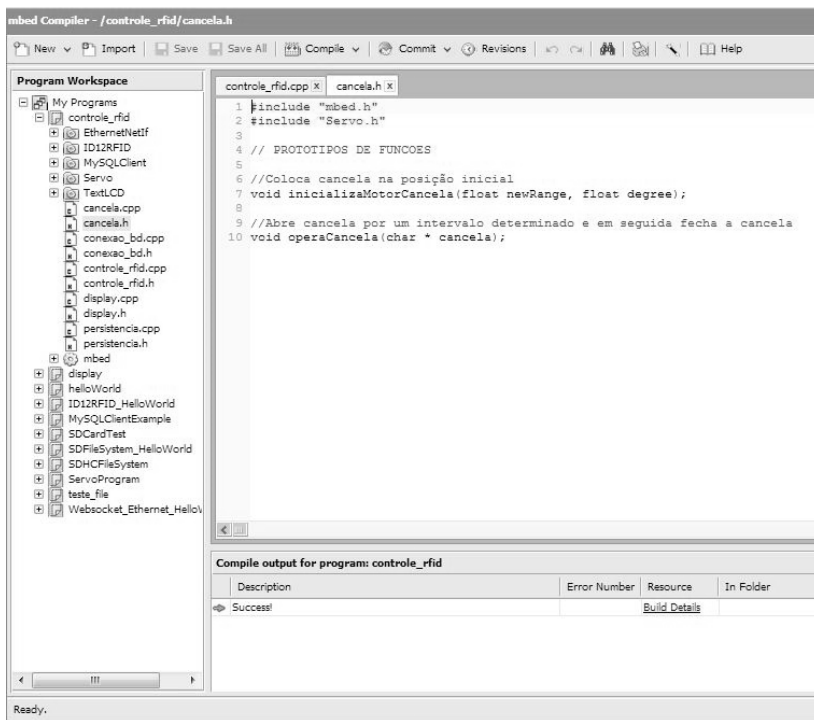


FIGURA 4.1 - Interface de desenvolvimento.

Para o desenvolvimento da aplicação web optou-se pela linguagem de programação PHP (*Personal Home Page*), por ser *open source*, ter ampla utilização e poder ser mesclada dentro de código HTML (*HyperText Markup Language*). O editor de texto e de código fonte Notepad++ foi empregado como ferramenta de desenvolvimento da aplicação web.

MySQL é um servidor de banco de dados relacional e *open source* que utiliza a linguagem SQL (*Structured Query Language*). Por ser *open source*, apresentar bom desempenho e ser facilmente integrado ao PHP, foi escolhido para armazenar os dados da aplicação web.

O Apache foi escolhido como servidor web deste projeto, responsável por armazenar o código HTML e PHP. A fim de

agilizar o processo de instalação da infraestrutura para suporte à aplicação web, foi empregada a ferramenta *Easy PHP*. Essa inclui servidor Apache, banco de dados MySQL e PHPMyAdmin⁵.

Durante o desenvolvimento da aplicação web, verificou-se que não seria possível utilizar a última versão do EasyPHP, sendo necessário adotar a versão EasyPHP 1.8.0.0, que possui as seguintes versões dos pacotes supracitados:

- Apache 1.3.33.
- PHP 4.3.10.
- PHPMyAdmin 2.6.1.
- MySQL 4.1.9.

Essa limitação na versão do EasyPHP ocorreu devido a biblioteca responsável pela comunicação entre o microcontrolador e o banco de dados não ser compatível com versões do MySQL superiores a 4.1. Considerando que não havia outra biblioteca disponível e que a implementação de uma para substituí-la implicaria em um custo não previsto, que poderia inviabilizar a conclusão do desenvolvimento no prazo estabelecido, optou-se por adotar a versão citada, validando o protótipo. Maiores informações sobre as bibliotecas empregadas serão apresentadas na próxima seção.

A ferramenta *CA ERwin Data Modeler*, versão 9.0.00.3711, foi utilizada para elaboração do modelo lógico do banco de dados.

Para o projeto do hardware, foi adotado o Proteus 7.8 Professional, um conjunto de ferramentas de EDA (*Electronic Design Automation*) que combina ambiente de simulação de circuitos eletrônicos e de *design* de circuito impresso. O ISIS (*Intelligent Schematic Input System*) foi utilizado para criar o esquemático enquanto o *layout* da placa de circuito impresso foi

⁵ PHPMyAdmin – ferramenta web desenvolvida em PHP que permite administrar o MySQL pela internet.

desenhado utilizando o ARES (*Advanced Routing and Editing Software*). O Proteus também permite efetuar simulação através do esquemático elaborado, todavia não foi possível realizá-la, pois o programa não dispõe do microcontrolador e do leitor RFID empregados no projeto.

4.2 Descrição do software

A seguir é detalhado o software desenvolvido neste projeto. Com o intuito de facilitar a compreensão, a descrição é dividida em dois módulos: aplicação web e sistema microcontrolado.

Aplicação Web

O desenvolvimento do módulo *web* foi iniciado com a definição do modelo lógico para a base de dados. Na Figura 4.2 é apresentada a modelagem da base de dados, para a qual foram criadas três tabelas: *Funcionario*, *Veiculo* e *Acesso*.

Considerou-se que um funcionário poderá ter zero ou muitos registros, assim como zero ou muitos veículos. Entretanto, um registro e um veículo poderão ter somente um funcionário associado, logo as tabelas *Acesso* e *Veiculo* possuem chaves estrangeiras⁶ da tabela *Funcionario*.

Na tabela *Funcionario*, a chave primária é o identificador da etiqueta que lhe foi entregue, logo se considera que não será necessário exigir do funcionário a etiqueta em caso de demissão, basta removê-la da lista de identificadores autorizados. O mesmo deve ser feito em caso de roubo ou perda.

⁶ Chave estrangeira (FK – Foreign Key) é um atributo de uma determinada tabela que aponta para a chave primária de outra tabela, caracterizando um relacionamento entre essas tabelas.

Na tabela Acesso, o campo tipo_acesso indica se o registro é uma tentativa de entrada ou saída. E o campo resultado permite ao administrador verificar se esse registro foi autorizado ou bloqueado.

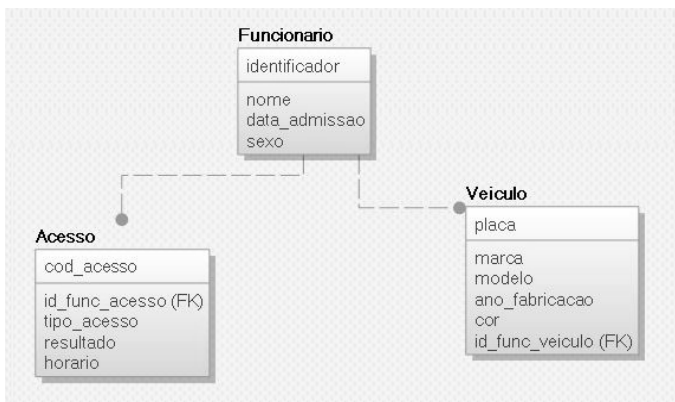


FIGURA 4.2 - Modelo lógico da base de dados.

O Apêndice A apresenta os SQLs utilizados para criação das tabelas e do usuário para acesso a base de dados.

A aplicação web tem por objetivo disponibilizar uma ferramenta ao usuário para cadastro, edição e exclusão de veículos e funcionários, além de possibilitar a consulta dos registros de entrada e saída obtidos pelo microcontrolador.

Na Figura 4.3 é apresentada a tela inicial do sistema, que se divide em quatro módulos: cabeçalho, menu, rodapé e centro. Sendo que o centro é dinâmico, ou seja, seu conteúdo é alterado conforme o item do menu selecionado pelo usuário.



FIGURA 4.3 - Sistema de Controle de Estacionamento RFID - Tela Principal.

Para conexão com o banco de dados, é utilizado o arquivo config.php, que armazena as seguintes configurações: servidor, usuário, senha e base de dados. Assim que o sistema é totalmente carregado, é estabelecida a conexão com o banco de dados baseado nessas informações.

Na Figura 4.4 é apresentada a tela de cadastro de funcionários. No campo identificador, o usuário deve inserir o ID da etiqueta que foi entregue ao funcionário que está sendo cadastrado.

Identificador	<input type="text"/>
Nome	<input type="text"/>
Data de Admissão	<input type="text" value="01"/> <input type="text" value="01"/> <input type="text" value="1980"/>
Sexo	<input checked="" type="radio"/> Masculino <input type="radio"/> Feminino
	<input type="button" value="Salvar"/>

FIGURA 4.4 - Tela para Cadastro de Funcionário.

A Figura 4.5 corresponde à tela que será apresentada quando o usuário selecionar o item Listar Funcionários. Quando a ação Editar é selecionada, é apresentada a mesma tela do cadastro de funcionário com os campos preenchidos, porém neste caso o campo Identificador não pode ser alterado, visto que é a chave primária do Funcionário. Para um funcionário ser excluído da base de dados, ele não pode possuir nenhum Acesso ou Veículo associado ao seu identificador, caso contrário seria gerada uma inconsistência na base de dados.

Ações	Identificador	Nome	Data de Admissao	Sexo
[Editar] [Excluir]	9643059	João da Silva	01/08/1983	Masculino
[Editar] [Excluir]	7654321	Karla Maria Garcia	17/08/1983	Feminino

FIGURA 4.5 – Tela para Listar Funcionários.

Na Figura 4.6 é apresentada a tela para cadastro dos veículos. No campo Funcionário, são listados automaticamente os funcionários já cadastrados e o identificador correspondente, a fim de agilizar o cadastro do veículo.

Placa	<input type="text"/>
Marca	<input type="text"/>
Modelo	<input type="text"/>
Ano de Fabricacao	<input type="text"/>
Cor	<input type="text"/>
Funcionario	João da Silva - 9643059 ▼
<input type="button" value="Salvar"/>	

FIGURA 4.6 – Tela para Cadastro de Veículos.

A Figura 4.7 corresponde à tela que é apresentada quando o usuário seleciona no menu o item Listar Veículos. Quando a ação Editar é selecionada, é apresentada a mesma tela do cadastro de veículos com os campos preenchidos, porém neste

caso o campo Placa não pode ser alterado, visto que é a chave primária do Veículo. A opção Excluir permite eliminar da base de dados o veículo selecionado.

Ações	Placa	Marca	Modelo	Ano de Fabricacao	Cor	Funcionario
[Editar] [Excluir]	MIW9737	Chevrolet	Celta	2011	Prata	9643059

FIGURA 4.7 - Tela para Listar Veículos.

Na Figura 4.8 é apresentada a tela que é mostrada ao usuário quando ele seleciona no menu a opção Listar Registros. Deve ser selecionada a data, o horário inicial e o final do período que se deseja pesquisar um determinado registro.

Data Inicio	01 ▾	01 ▾	2011 ▾
Horario Inicio	00 ▾	00 ▾	00 ▾
Data Fim	01 ▾	01 ▾	2013 ▾
Horario Fim	00 ▾	00 ▾	00 ▾
<input type="button" value="Listar"/>			

FIGURA 4.8 - Tela para Listar Registros.

Na Figura 4.9 é apresentado um exemplo de visualização das informações de registros encontradas no período especificado.

Horario	Tipo de Acesso	Resultado	Identificador Funcionario	Nome Funcionario
2013-04-21 09:46:07	entrada	sucesso	9643059	João da Silva
2013-04-21 09:46:13	entrada	sucesso	9643059	João da Silva
2013-04-21 15:03:28	entrada	sucesso	9643059	João da Silva
2013-04-21 15:09:50	entrada	falha_lotado	9643059	João da Silva
2013-06-12 20:42:22	saida	sucesso	9643059	João da Silva
2013-06-12 20:42:33	saida	sucesso	9643059	João da Silva
2013-06-12 20:42:43	entrada	sucesso	9643059	João da Silva
2013-06-12 20:42:54	entrada	sucesso	9643059	João da Silva
2013-06-12 20:43:17	saida	sucesso	9643059	João da Silva
2013-06-12 20:43:28	entrada	sucesso	9643059	João da Silva

FIGURA 4.9 - Tela Relação de Registros de Acesso.

Sistema Microcontrolado

Uma das principais vantagens do emprego da Mbed são as várias bibliotecas disponibilizadas pela comunidade de usuários, que possibilitam otimizar o tempo na programação de itens auxiliares. Na Figura 4.2 são apresentados os dispositivos necessários para compor a solução de controle de estacionamento por RFID e o tipo de saída que cada um utiliza no microcontrolador.

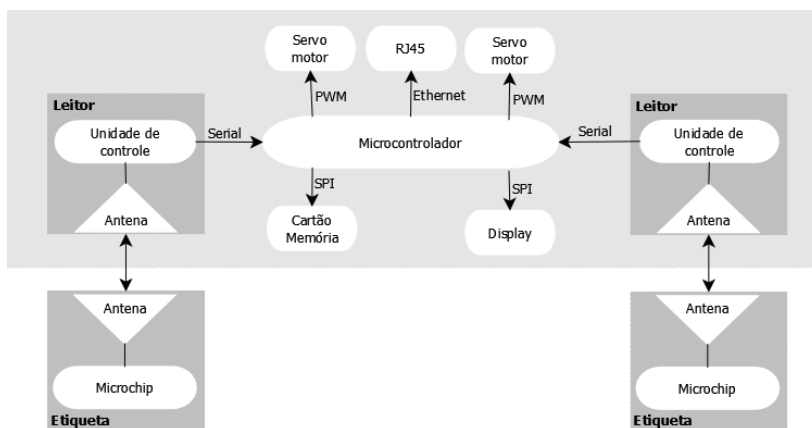


FIGURA 4.10 - Dispositivos auxiliares ao microcontrolador.

O projeto Mbed disponibiliza bibliotecas para controle de *display* LCD (*Liquid Crystal Display*), cartão de memória, servomotores, ethernet e leitor de radiofrequência. A seguir são listadas as bibliotecas utilizadas:

- **Mbed:** o objetivo da biblioteca mbed é fornecer abstração para o hardware do microcontrolador. O núcleo da biblioteca mbed disponibiliza uma API para controlar interfaces do microcontrolador, além de outras inicializações e funções em tempo de execução que auxiliam na criação de programas.
- **Servo:** essa biblioteca permite controlar um servomotor através de um sinal PWM e fornece controle do servo entre mínimo e máximo configurando-o para 0,0 – 1,0. Como cada servomotor pode responder de forma diferente, ela disponibiliza uma função para calibrar esse intervalo, logo 0,0 – 1,0 é a faixa limite do servo.
- **EthernetNetIf:** permite associar à interface de rede um endereço IP (*Internet Protocol*) estático ou utilizar DHCP (*Dynamic Host Configuration Protocol*). Neste projeto, optou-se pelo DHCP devido à praticidade, pois dispensa a necessidade de consultar endereços IPs disponíveis e torna o sistema independente de rede. Essa biblioteca é baseada na pilha TCP/IP lwIP⁷ que foi portada para a MBED.
- **ID12RFID:** essa biblioteca é específica para o leitor RFID adotado neste projeto, o ID12. Após configurar um pino de saída serial, o identificador capturado pelo leitor no formato de 32 bits é passado pela biblioteca para a aplicação como um inteiro.
- **TextLCD:** biblioteca para painéis LCD baseados no chip HD77780. Suporta vários modelos de painéis: 16 x 2,

⁷ lwIP (*Lightweight TCP/IP stack*) é uma pilha TCP/IP *open-source* desenvolvida para sistemas embarcados com foco na redução do uso de recursos.

16 x 4, 20 x 2, 20 x 4 entre outros, sendo que neste projeto é empregado o modelo 20 x 4.

- **MySQLClient:** essa biblioteca foi utilizada para permitir a comunicação do microcontrolador com o banco de dados MySQL. Essa biblioteca permite executar um conjunto limitado de requisições SQL sobre um servidor MySQL com versão igual ou superior a 4.1. Porém, durante o desenvolvimento do projeto verificou-se que ela não tem suporte a consultas, o que provocou grande impacto no projeto, pois inicialmente pretendia-se pesquisar os identificadores com autorização de acesso no banco de dados, e diante desta limitação, não foi possível.

Na Figura 4.11 é apresentada a estrutura de arquivos desenvolvida na elaboração do sistema de controle de estacionamentos por radiofrequência. Para cada arquivo com extensão `cpp` há um arquivo *header* identificado pela extensão `.h`, utilizados para declarar tipos, variáveis, macros e protótipos de funções.

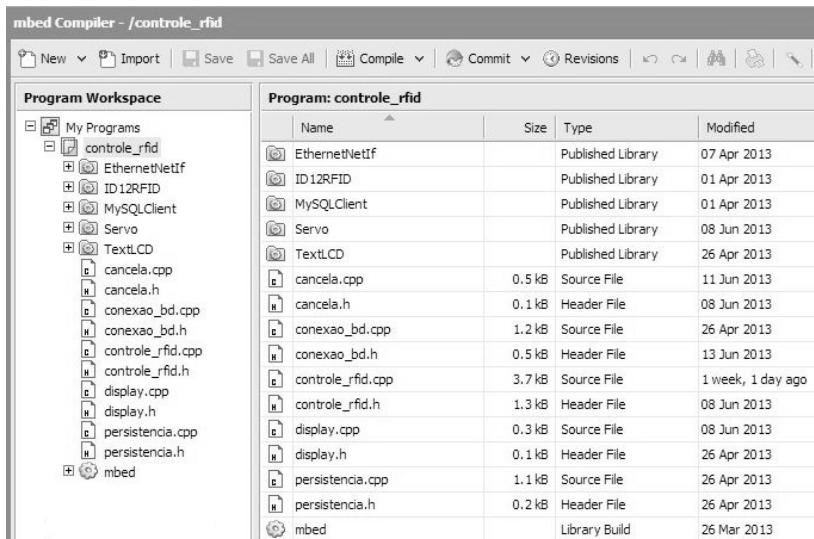


FIGURA 4.11 - Arquivos do sistema de controle RFID.

A seguir são listados os arquivos descrevendo suas funcionalidades.

- persistencia.c e persistencia.h:** conforme informado no capítulo anterior, o microcontrolador armazena um arquivo com a lista de identificadores que possuem permissão de acesso e outro arquivo com a quantidade de vagas livres. O módulo de persistência é responsável por ler esses arquivos, disponibilizando em memória os dados que armazenam. Ele também atualiza em arquivo a quantidade de vagas livres, sempre que esta é modificada. Na Figura 4.12 são apresentados os protótipos de funções disponíveis neste módulo. O parâmetro *limite*, presente na função *carregaVariáveis*, representa a quantidade máxima de identificadores que o sistema poderá ter cadastrado; atualmente esse valor não pode ser superior a 4771, pois excederá a capacidade máxima da RAM que é de 32 kB.

```
#include "mbed.h"
#include <stdio.h>
#include <stdlib.h>

// PROTOTIPOS DE FUNCOES

//Lê o arquivo com os identificadores e com a quantidade de vagas
livres
int carregaVariaveis(int *identificadores, int *qtdaVagasLivres, int
limite);

//Atualiza arquivo com quantidade de vagas livres
void atualizaVagasLivres(int qtdaVagasLivres);
```

FIGURA 4.12 – Conteúdo do arquivo persistencia.h.

- **display.c e display.h:** utiliza a biblioteca TextLCD para configurar os pinos do microcontrolador que são utilizados para comunicação com o display, assim como implementa a função responsável pela escrita no mesmo. Na Figura 4.13 é apresentado o protótipo de função responsável pela atualização do *display*.

```
#include "mbed.h"
#include "TextLCD.h"

// PROTOTIPOS DE FUNCOES

//Atualiza mensagem apresentada no display
void atualizaDisplay(char *msgDisplay);
```

FIGURA 4.13 - Conteúdo do arquivo display.h.

- **cancela.c e cancela.h:** emprega a biblioteca Servo. É utilizada na inicialização do sistema para colocar o servomotor na posição inicial (cancela fechada). Além

disto, possui a função *operaCancela* que é acionada sempre que um usuário entrar ou sair do estacionamento. Esta função move o servo para a posição que representa a cancela aberta, mantém essa posição por um determinado intervalo de tempo e em seguida volta o servo para a posição original, representando o fechamento da cancela. Na Figura 4.14 são apresentados os protótipos de funções referentes à cancela.

```
#include "mbed.h"
#include "Servo.h"

// PROTOTIPOS DE FUNCOES

//Coloca cancela na posição inicial
void inicializaMotorCancela(float newRange, float degree);

//Abre cancela por um intervalo determinado e em seguida fecha a
cancela
void operaCancela(char * cancela);
```

FIGURA 4.14 - Conteúdo do arquivo cancela.h.

- **conexao_bd.c e conexao_bd.h:** utiliza a biblioteca MySQLClient. É responsável pela conexão com o banco de dados, assim como pela definição das informações necessárias para o estabelecimento da conexão: IP do servidor, porta, usuário, senha e base de dados. A conexão é criada a cada nova requisição SQL para a base de dados, sendo encerrada quando a requisição é concluída. Esse módulo utiliza uma função *callback*, disponibilizada pela biblioteca, que lhe permite avaliar o resultado das requisições. Se for solicitado o envio de uma requisição para o banco de dados e a rede de dados estiver indisponível, a função *callback* retorna uma falha e o registro não será armazenado no banco de dados, mas o sistema continua operando normalmente. Na Figura 4.15 são apresentados os protótipos de funções referentes à conexão com o banco de dados.

```

#include "mbed.h"
#include "MySQLClient.h"

//DEFINICOES
#define SQL_SERVER "192.168.25.5"
#define SQL_PORT 3306
#define SQL_USER "rfid"
#define SQL_PASSWORD "12345"
#define SQL_DB "controle_rfid"

//PROTOTOPOS DE FUNCOES

//Lib MySQLClient permite utilizar funcao de callback que informa o
estado da requisicao
void retornoRequisicao(MySQLResult retorno);

//Insere no banco de dados o registro de acesso
void insereRegistroBancoDados(int identificador, char *tipo_acesso,
char *resultado_acesso);

```

FIGURA 4.15 - Conteúdo do arquivo conexao_bd.h.

- **controle_rfid.c e controle_rfid.h:** utiliza as bibliotecas ID12RFID e EthernetNetIf. É o módulo principal, possui a função *“main”*, sendo responsável pela inicialização do sistema e acionamento dos demais módulos, além de efetuar o tratamento dos identificadores informados pelos leitores RFID. Assim que o sistema é ligado, a rede de dados é inicializada, sendo que uma variável indica se foi possível estabelecer conexão. Em seguida, os arquivos com a lista de identificadores e quantidade de vagas disponíveis são carregados em memória e o display é atualizado. O próximo passo é a inicialização dos leitores RFID, sendo realizada a configuração dos pinos do microcontrolador que são utilizados e iniciado o processo de monitoramento dos leitores. Assim que um dos leitores informar um identificador, o sistema identifica qual leitor está realizando a comunicação (entrada ou saída) e inicia o procedimento de entrada ou saída apresentado no capítulo anterior nas Figuras 3.3 e 3.4.

Na Figura 4.16 são apresentados os protótipos de funções referentes a esse módulo.

```
#include <stdio.h>
#include "mbed.h"
#include "ID12RFID.h"
#include "EthernetNetIf.h"
#include "conexao_bd.h"
#include "persistencia.h"
#include "display.h"
#include "cancela.h"

// DEFINICOES
#define pinoSensorSaida p27
#define pinoSensorEntrada p14

//Limite máximo de vagas
#define LIMITE_VAGAS 2000

typedef enum {entrada,saida} tipos_acesso;
typedef enum {sucesso,falha_lotado, falha_idnaoreg} resultados_acesso;

// ESTRUTURA DE DADOS
//Armazena o tipo de acesso (entrada ou saida) e o resultado deste para
depois poder atualizar o banco
typedef struct {
    tipos_acesso tipo_acesso;
    resultados_acesso resultado_acesso;
} acesso;

// PROTOTIPOS DE FUNCOES

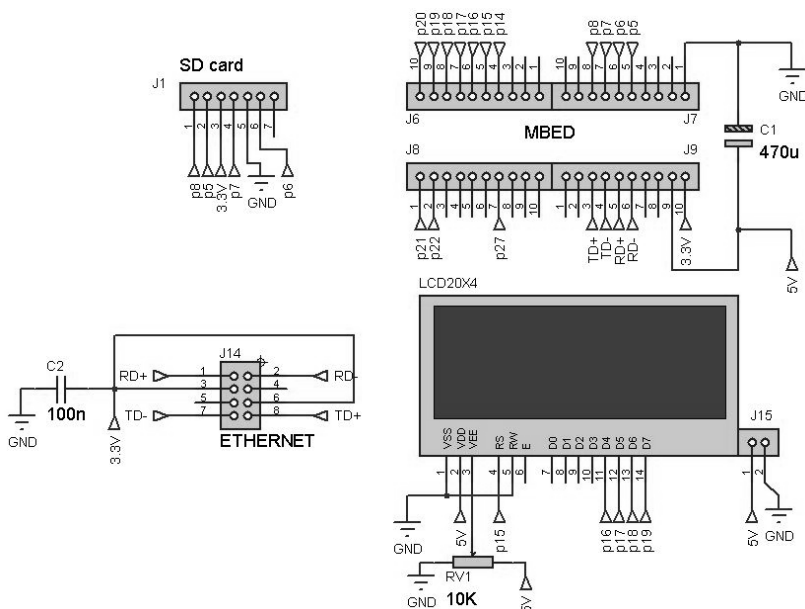
//Conecta mbed na rede
void inicializaRede();
//Inicializa as variaveis globais
int inicializaVariaveis();
/* Inicializa e monitora os sensores RFID, quando receber um ID aciona o
sistema para trata-lo */
void monitoraSensores();
/* Verifica permissões de acesso do cliente, acionar cancela, atualizar
display e BD */
void trataID(int identificador, tipos_acesso tipo_acesso);
//Procura no array o ID fornecido pelo sensor RFID
int busca(int busca);
//Funcao auxiliar para ordenar os ID carregados do arquivo na flash
int compare (const void * a, const void * b);
```

FIGURA 4.16 - Conteúdo do arquivo controle_rfid.h.

Após a conclusão do desenvolvimento do *firmware*, ele foi compilado através da IDE *Compiler Mbed*. Para gravação do *firmware*, copiava-se o binário gerado para o driver, criado automaticamente ao conectar a Mbed no computador, e reiniciava-se a placa.

4.3 Descrição do hardware

A elaboração do projeto de hardware consistiu basicamente na conexão dos componentes escolhidos, conforme Capítulo 3, ao microcontrolador. Na Figura 4.17 são apresentados os circuitos eletrônicos referentes à interligação do microcontrolador ao SD card, Ethernet e display.



Na Figura 4.18 são apresentados os circuitos referentes à interligação do microcontrolador aos servomotores e leitores RFID.

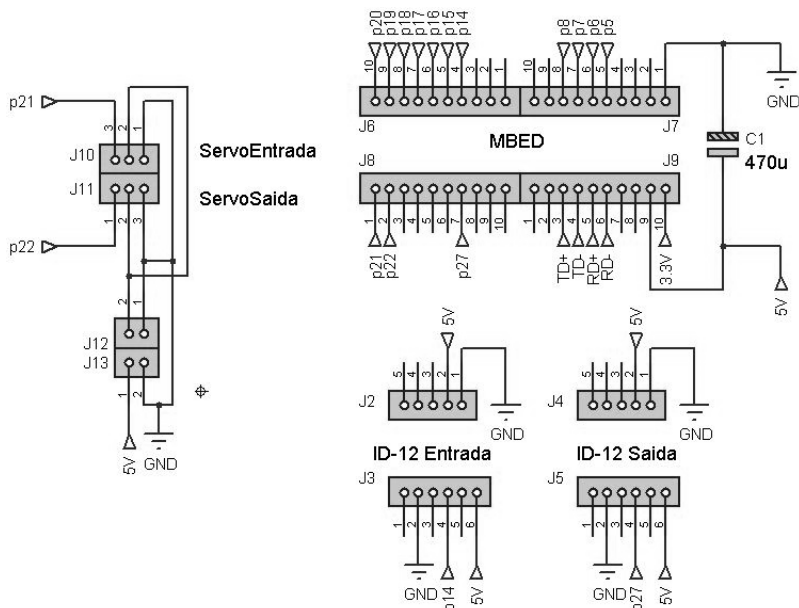


FIGURA 4.18 – Interligação do microcontrolador aos servomotores e leitores RFID .

Para corrigir oscilações na alimentação quando o ID-12 realizava a leitura de uma etiqueta, foi necessário utilizar um capacitor entre a alimentação (5 V) e a referência do circuito.

No circuito de alimentação dos servomotores, optou-se por deixar opcional a alimentação desses. O usuário pode escolher entre o 5 V, fornecido pela Mbed, ou colocar uma bateria externa. Essa escolha foi tomada, porque durante testes verificou-se que a USB não consegue fornecer corrente necessária para operação dos servomotores.

Inicialmente, o circuito eletrônico foi montado e testado em uma placa de ensaio. Após confirmar o funcionamento, o projeto

foi encaminhado a uma empresa para confecção da placa. Na Figura 4.19 é apresentado o layout da placa, elaborado através do módulo ARES do Proteus. Nos espaços indicados com os números 1, 2, 3 e 4 serão conectados o módulo MicroSDcard, o display, leitor RFID de entrada e leitor RFID de saída, respectivamente.

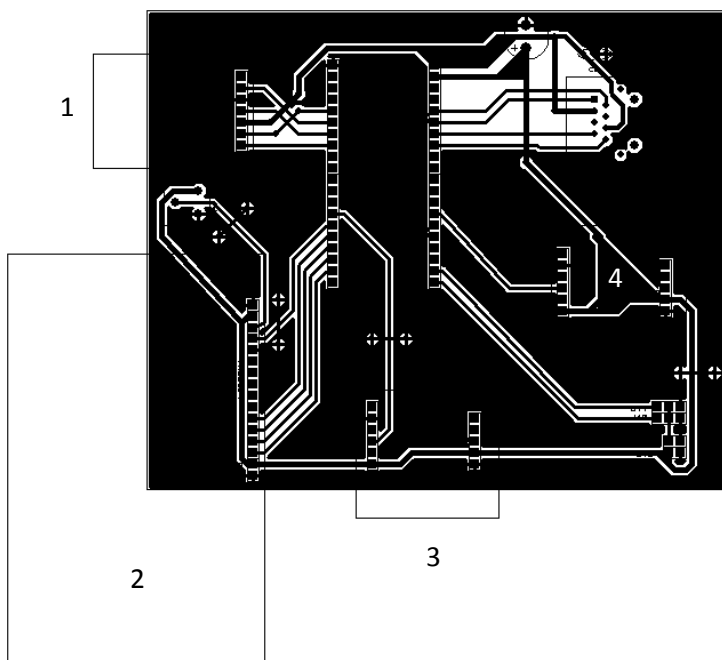


FIGURA 4.19 - Layout do projeto.

Devido à simplicidade do *layout*, optou-se pela elaboração de uma placa face simples, porém tornou-se necessário o emprego de algumas pontes utilizando fios, como *jumpers*.

Na Figura 4.20 é apresentada a placa desenvolvida. Nessa imagem foi utilizado apenas um servomotor, que representa a cancela de entrada, sendo alimentado por 4 pilhas em série de

1,5 V cada, pois o microcontrolador estava sendo alimentado via USB.

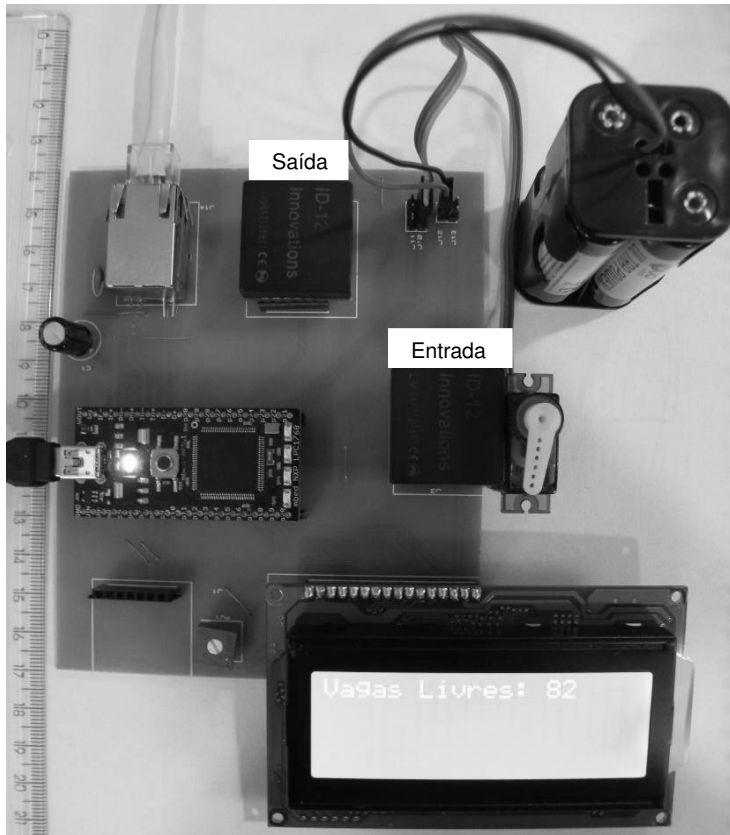


FIGURA 4.20 – Protótipo desenvolvido.

Sendo que este trabalho consistiu no desenvolvimento de um protótipo, não foi necessário preocupar-se com a distância entre o microcontrolador e os leitores RFID. Porém, considerando que a transmissão do identificador entre leitores e microcontrolador é realizada via RS232 a uma taxa de 9600 bps, em um cenário real a distância máxima entre microcontrolador e leitores não poderá exceder 15 metros (TURNER e

KOMARINSKI, 2003). Logo o sistema somente atende cenários nos quais as cancelas de entrada e saída estejam no máximo 30 metros distantes entre si.

Até a conclusão do projeto, o módulo para leitura e gravação do cartão de memória adquirido não foi entregue, logo os arquivos com a relação de identificadores com permissão de acesso e o arquivo com a quantidade de vagas livres foram armazenados em memória *flash*.

4.4 Custos do projeto

Os custos envolvidos no desenvolvimento do projeto consistem da aquisição dos componentes utilizados e da confecção da placa. Na Tabela 4.1 são apresentados os principais itens adquiridos para confecção do protótipo e seus respectivos custos.

TABELA 4.1 - Principais custos de hardware do projeto.

Item	Descrição	Quantidade	Preço unitário (R\$)
Mbed	Embarcar o software implementado	1	190,00
ID12	Leitura das etiquetas	2	60,00
Etiquetas	Simular os acessos	2	2,00
Módulo do cartão de memória	Gravar o cartão de memória	1	25,00
Display	Informar quantidade de vagas livres	1	30,00
RJ45	Permite acesso a rede de dados	1	4,00
Servomotor	Simular as cancelas	2	15,00
Placa	Confecção da placa	1	43,25
Custo Total	-	11	446,25

5. TESTES REALIZADOS E RESULTADOS

A seguir são apresentados os testes realizados para avaliar o funcionamento do protótipo e os resultados obtidos. Para realização dos testes considerou-se um estacionamento com capacidade máxima de 100 vagas, sendo que na configuração inicial do sistema o estacionamento deve estar com todas as vagas livres.

1. Estando o sistema com 100 vagas livres e conectado a internet, foi apresentada ao leitor de entrada uma etiqueta cujo identificador possuía permissão de acesso.

Resultado: Display foi atualizado para 99 vagas livres, cancela de entrada foi aberta e um registro de entrada foi inserido no banco de dados. Nas Figuras 5.1 e 5.2 são apresentados o display com a informação sobre as vagas livres e o registro de acesso na aplicação web, respectivamente.

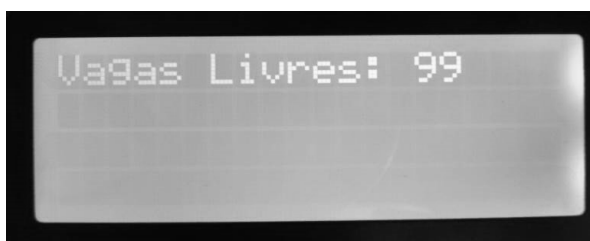


FIGURA 5.1 - Display informando quantidade de vagas.

Horario	Tipo de Acesso	Resultado	Identificador Funcionario	Nome Funcionario
2013-10-05 16:15:38	entrada	sucesso	9643059	João da Silva

FIGURA 5.2 - Registro de acesso com sucesso.

2. Estando o sistema com 100 vagas livres e conectado a internet, foi apresentada ao leitor de entrada uma etiqueta cujo identificador não possuía permissão de acesso.

Resultado: Por cinco segundos o display apresentou a mensagem “Usuário não autorizado”, após voltou a apresentar a quantidade de vagas livres. Na Figura 5.3 é apresentado o display com a informação de usuário não autorizado.

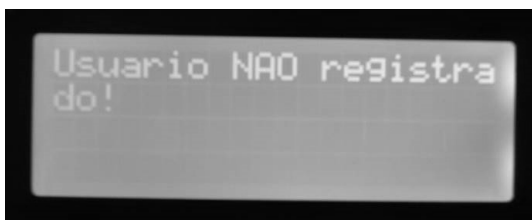


FIGURA 5.1 - Display informando acesso não autorizado.

3. Estando o sistema com 100 vagas livres e sem conexão com a internet, foi apresentada ao leitor de entrada uma etiqueta cujo identificador possuía permissão de acesso.

Resultado: Display foi atualizado para 99 vagas livres, cancela de entrada foi aberta e nenhum registro foi inserido no banco de dados.

4. Estando o sistema com uma vaga livre e conectado a internet, foi apresentada ao leitor de entrada uma etiqueta cujo identificador possuía permissão de acesso.

Resultado: Display foi atualizado para “Lotado”, cancela de entrada foi aberta e um registro de entrada foi inserido no banco de dados. Na Figura 5.4 é apresentado o display com a informação de lotado.

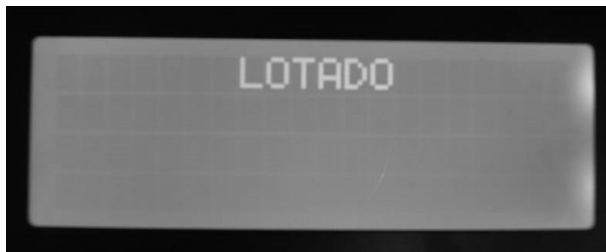


FIGURA 5.2 - Display informando LOTADO

5. Estando o sistema com 0 (zero) vagas livres e conectado a internet, foi apresentada ao leitor de entrada uma etiqueta cujo identificador possuía permissão de acesso.

Resultado: Display permaneceu informando “Lotado” e um registro de falha na tentativa de entrada foi inserido no banco de dados. Na Figura 5.5 é apresentado o registro de falha na entrada devido ao estacionamento estar lotado.

Horario	Tipo de Acesso	Resultado	Identificador Funcionario	Nome Funcionario
2013-10-05 17:08:19	entrada	sucesso	9643059	João da Silva
2013-10-05 17:08:40	entrada	falha_lotado	1128052	José da Silva

FIGURA 5.3 - Registro de falha na entrada.

6. Estando o sistema com 0 (zero) vagas livres e conectado a internet, foi apresentada ao leitor de saída uma etiqueta cujo identificador possuía permissão de acesso.

Resultado: Display foi atualizado de “Lotado” para “Vagas Livres: 1”, cancela de saída foi aberta e um registro de saída foi inserido no banco de dados. Na Figura 5.6 é apresentado o registro de saída na aplicação web.

Horario	Tipo de Acesso	Resultado	Identificador Funcionario	Nome Funcionario
2013-10-05 17:08:19	entrada	sucesso	9643059	João da Silva
2013-10-05 17:08:40	entrada	falha_lotado	1128052	José da Silva
2013-10-05 17:10:16	saida	sucesso	9643059	João da Silva

FIGURA 5.4 - Registro de saída.

7. Estando o sistema com uma vaga livre e conectado a internet, foi apresentada ao leitor de saída uma etiqueta cujo identificador não possuía permissão de acesso.

Resultado: Nenhuma ação é executada.

8. Estando o sistema com 50 vagas livres e conectado a internet, foram apresentadas simultaneamente aos leitores de entrada e saída etiquetas cujos identificadores possuíam permissão de acesso.

Resultado: Procedimentos de entrada (atualização do display, operação da cancela e registro no banco de dados) e saída (operação da cancela e registro no banco de dados) foram executados com sucesso, um em sequência ao outro. Porém foi possível observar que a ordem de execução dos procedimentos varia conforme o microcontrolador realiza a leitura do identificador enviado pelos leitores RFID. Também foi observado que, mesmo as etiquetas sendo apresentadas simultaneamente, os registros no banco de dados apresentam um intervalo de 10 segundos, tempo necessário para o microcontrolador efetuar a verificação de acesso, movimentar a cancela (que fica 5 segundos aberta) e enviar o registro ao banco. Na Figura 5.7 são apresentados os registros de entrada e saída quando as etiquetas são apresentadas simultaneamente nos leitores.

Horario	Tipo de Acesso	Resultado	Identificador Funcionario	Nome Funcionario
2013-10-05 17:17:09	entrada	sucesso	1128052	José da Silva
2013-10-05 17:17:24	entrada	sucesso	9643059	João da Silva
2013-10-05 17:17:34	saida	sucesso	1128052	José da Silva

FIGURA 5.5 - Registros de entrada e saída

9. Estando o sistema com 50 vagas livres, metade da sua capacidade máxima, o mesmo foi reiniciado.

Resultado: Após a reinicialização do sistema o display voltou a apresentar 50 vagas livres e os procedimentos de entrada e saída permaneceram sendo executados com sucesso.

Através dos testes realizados acima, além dos resultados já apresentados, também foi possível observar que devido à relativa proximidade dos leitores no protótipo desenvolvido, observou-se que algumas vezes uma etiqueta é apresentada ao leitor de entrada e lida pelo leitor de saída, por exemplo. Isso se deve ao fato de não ter respeitada a distância mínima de 12 cm entre os leitores. Porém como no produto final os leitores sempre estão distantes entre si o problema não se manifestará.

Como resultado dos testes também foi possível identificar a necessidade de acrescentar um display na cancela de saída, pois no caso de uma tentativa de saída por uma etiqueta não autorizada, o operador do sistema pode ficar em dúvida se a cancela não é aberta por falha no sistema ou por não possuir autorização.

Em relação ao sistema web foram realizados testes de cadastro, edição, exclusão e consulta de funcionários e veículos com sucesso. A consulta de registro também apresentou corretamente os registros enviados pelo microcontrolador, conforme apresentado nas Figuras 5.2, 5.5, 5.6 e 5.7.

6. CONCLUSÕES E SUGESTÕES PARA TRABALHOS FUTUROS

A tecnologia RFID está paulatinamente substituindo os códigos de barras. Ela pode ser aplicada em diversas soluções, principalmente em cadeias de suprimentos para controles de estoques, no controle de animais e também no controle de acesso, conforme abordado neste projeto.

Os testes realizados com o protótipo desenvolvido permitiram confirmar que o sistema realiza corretamente o controle de acesso e o gerenciamento da quantidade de vagas, bloqueando acesso no caso de usuários não autorizados ou de estacionamento lotado. O display na entrada orienta os usuários sobre a disponibilidade de vagas e usuários não autorizados. A aplicação web também atendeu as necessidades, possibilitando cadastro, exclusão, edição e consulta de funcionários e veículos, bem como consulta dos registros inseridos no banco de dados pelo microcontrolador.

Todavia, para o uso comercial fazem-se necessárias alterações tanto no hardware como no software. No projeto de hardware, deve-se considerar que as cancelas estarão fisicamente distantes entre si, logo os leitores RFID não estão na mesma placa. A inserção de um display no portão de saída melhoraria a interação com o usuário, principalmente para indicar uma tentativa de saída com etiqueta sem permissão. Em relação ao software, primeiramente deve-se efetuar o desenvolvimento do armazenamento de informações no cartão de memória, este módulo não foi implementado, visto que o hardware adquirido não foi entregue em tempo. As configurações do banco de dados são *hard code*, logo o sistema deve ser alterado para armazená-las de forma a permitir que o usuário modifique-as, como por exemplo, criando um arquivo de configurações que possa ser editado e lido pelo sistema. Também é interessante proteger o acesso à aplicação web através de *login* e senha.

REFERÊNCIAS

ALMEIDA, Lucas Cavalcante de. **Aplicações Da Tecnologia De Identificação Por Radiofrequência – Rfid**. 2011. 98 f.. Monografia (Bacharelado em Engenharia de Teleinformática) – Centro de Tecnologia, Universidade Federal do Ceará, Fortaleza. Disponível em: http://www.cgeti.deti.ufc.br/monografias/LUCAS_CAVALCANTE_DE_ALMEIDA.pdf. Acesso em: 19 jun. 2013.

DIAS, João Filipe Ferreira. **Desenvolvimento de Aplicações para Sistemas RFID Comerciais**. 2008. 120 f.. Dissertação (Mestrado em Engenharia Eletrônica Industrial e de Computadores) – Escola de Engenharia, Universidade do Minho. Disponível em: <http://intranet.dei.uminho.pt/gdmi/galeria/temas/pdf/.pdf>. Acesso em: 9 jun. 2013.

FINKENZELLER, Klaus. **RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication**. Traduzido para o inglês por Dorte Muller. 3 ed. Chippenharn: Wiley, 2010, 462 p.

GAO RFID Inc. **RFID Solutions for ID Badges and Access Control**. Disponível em: <http://accesscontrol.gaorfid.com/>. Acesso em: 12 fev. 2013.

GOMES, Hugo Miguel Cravo. **Construção de um Sistema RFID com Fins de Localização Especiais**. 2007. 91 f.. Dissertação (Mestrado em Engenharia e Telecomunicações) – Universidade de Aveiro. Disponível em: http://www.av.it.pt/nbcarvalho/docs/msc_hcg.pdf. Acesso em: 11 jun. 2013.

HAVER, Torstein. **Security and Privacy in RFID Applications**. 2006. 106 f.. *Master of Science in Communication Technology*. Norwegian University of Science and Technology Department of Telematics. Disponível em: <http://ntnu.diva-portal.org/smash/record.jsf?pid=diva2:348192>. Acesso em: 2 jun 2013.

HODGES, Steve; HARRISON, Mark. **Desmystifying RFID: Principles and Practicibilities**. 2003. Auto-ID Centre Institute for Manufacturing, University of Cambridge, Cambridge. Disponível em: <http://news.autoidlabs.org/uploads/media/CAM-AUTOID-WH024.pdf>. Acesso em: 25 jun. 2013.

ID INNOVATIONS. **ID Series Datasheet**. Disponível em: <https://www.sparkfun.com/datasheets/Sensors/ID-12-Datasheet.pdf>. Acesso em: 14 jul. 2013.

JUNIOR, Alberto Wiltgen. **Projeto do Processamento Digital de TAG RFID Adequado à Norma ISO/IEC 18000-2**. 2010. 84 f.. Monografia (Bacharelado em Engenharia da Computação) – Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre. Disponível em: <http://www.lume.ufrgs.br/handle/10183/25602>. Acesso em: 26 jun. 2013.

LAHIRI, Sandip. **RFID Sourcebook**, 2005. 1 ed. Massachusetts: IBM Press, 2005, 304 p.

MBED. **Mbed Hardware**. Disponível em: <http://mbed.org/handbook/mbed-Hardware>. Acesso em: 17 jul. 2013.

-----, **Mbed-SDK**. Disponível em: <http://mbed.org/handbook/mbed-SDK>. Acesso em: 17 jul. 2013.

MONTEIRO, Fernando V; PACHECO, Gabriel F. C.; LIMA, Lucas C. **RFID: Radio Frequency Identification**. 2010. Universidade Federal do Rio de Janeiro, Rio de Janeiro. Disponível em: http://www.gta.ufrj.br/grad/10_1/rfid/index.html. Acesso em: 21 set. 2013.

NAEC; TEKES; FORMAS; DTI. **Review of the current state of Radio Frequency Identification (RFID) Technology, Its Use and Potential Future Use in Construction**. 2006. Disponível em: http://www.tekes.fi/fi/gateway/PTARGS_0_201_403_994_2095_43/http%3b/tekes-ali2%3b7087/publishedcontent/publish/programmes/rak_ymparisto/documents/report_rfid_in_construction.pdf. Acesso em: 9 jun. 2013.

OECD (2008). **Radio-Frequency Identification (RFID): A Focus on Information Security and Privacy**, OECD Digital Economy Papers, No. 138, OECD Publishing. Disponível em: <http://dx.doi.org/10.1787/230618820755>. Acesso em: 10 jul. 2013.

PALA, Zeydin; INANÇ, Nihat. **Smart Parking Applications Using RFID Technology**. IEEE, RFID Eurasia. 2007. Disponível em: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4368108&tag=1. Acesso em: 2 fev. 2013.

PEDRO, Luís Manuel Dias. **Plataforma de Comunicações sem Fios para Zigbee e RFID**, 95 f, 2008. Dissertação (Mestrado em Engenharia de Redes de Comunicações) – Instituto Superior Técnico – Universidade Técnica de Lisboa, Lisboa. Disponível em: <https://dspace.ist.utl.pt/bitstream/2295/230370/1/Tesfbuie%20Luis%20Pedro.pdf>. Acesso em: 4 jun. 2013.

KAISER, Aysha; KHAN, Shoab A. ***Automation of Time and Attendance using RFID Systems***. In: 2nd International Conference on Emerging Technologies, Peshawar, p. 60-63, nov. 2006. Disponível em: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4136896. Acesso em: 03 jun. 2013.

RADIO-ELECTRONICS. ***RFID Standarts***. Disponível em: <http://www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/iso-epcglobal-iec-standards.php>. Acesso em: 9 jun. 2013.

SHARMA, Meenakshi; SIDDIQUI, Adil. ***RFID Based Mobiles: Next Generation Applications***. In: 2nd IEEE International Conference on Information Management and Engineering (ICIME), 2010. Disponível em: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5477641. Acesso em: 2 jun. 2013.

SPARKFUN. ***Breakout Board for MicroSD Transflash***. Disponível em: <https://www.sparkfun.com/products/544>. Acesso em: 18 jul. 2013.

-----, ***RFID Reader ID-12***. Disponível em: <https://www.sparkfun.com/products/8419>. Acesso em: 14 jul. 2013.

-----, ***RFID Tag***. Disponível em: <https://www.sparkfun.com/products/8310>. Acesso em: 17 jul. 2013.

SWEENEY, Patrick J. ***RFID for Dummies***. Indianapolis: Wiley Publishing, 2005.

TURNER, Glen; KOMARINSKI, Mark F. ***Remote Serial Console HOWTO***. The Linux Document Project, 2003. Disponível em: <http://www.tldp.org/HOWTO/Remote-Serial-Console-HOWTO/>. Acesso em: 2 out. 2013.

WANBA, Samuel F.; KEATING, Byron; COLTMAN, Tim; MICHAEL, K. ***RFID Adoption Issues: Analysis of Organizational Benefits and Risks***, 2009. Auto ID Labs. Disponível em: <http://works.bepress.com/tcoltman/17/>. Acesso em: 2 jun. 2013.

APÊNDICES

APÊNDICE A – SQLs para criação das tabelas de dados

```
CREATE TABLE IF NOT EXISTS `controle_rfId`.`funcionario` (  
  `cod_funcionario` INT UNSIGNED NOT NULL ,  
  `nome_funcionario` VARCHAR(45) NOT NULL ,  
  `data_admissao` DATE NOT NULL ,  
  `sexo_funcionario` ENUM('M','F') NOT NULL ,  
  PRIMARY KEY (`cod_funcionario`))  
ENGINE = InnoDB;
```

```
CREATE TABLE IF NOT EXISTS `controle_rfId`.`acesso` (  
  `cod_acesso` INT UNSIGNED NOT NULL AUTO_INCREMENT ,  
  `horario` DATETIME NOT NULL ,  
  `tipo_acesso` ENUM ('entrada','saida') NOT NULL ,  
  `resultado` ENUM ('sucesso', 'lotado') NOT NULL ,  
  `id_func_acesso` INT UNSIGNED NOT NULL ,  
  PRIMARY KEY (`cod_acesso`) ,  
  INDEX `fk_id_func_acesso` (`id_func_acesso` ASC) ,  
  CONSTRAINT `fk_id_func_acesso`  
  FOREIGN KEY (`id_func_acesso` )  
  REFERENCES `controle_rfId`.`funcionario` (`cod_funcionario` )  
  ON DELETE NO ACTION  
  ON UPDATE NO ACTION)  
PRIMARY KEY (`cod_acesso`) ,  
ENGINE = InnoDB;
```

```
CREATE TABLE IF NOT EXISTS `controle_rfId`.`veiculo` (  
  `cod_veiculo` INT UNSIGNED NOT NULL AUTO_INCREMENT ,  
  `placa` VARCHAR(45) NOT NULL ,  
  `marca` VARCHAR(45) NOT NULL ,  
  `modelo` VARCHAR(45) NOT NULL ,  
  `ano_fabricacao` INT NOT NULL ,  
  `cor` VARCHAR(45) NOT NULL ,  
  `id_func_veiculo` INT UNSIGNED NOT NULL ,  
  PRIMARY KEY (`cod_veiculo`) ,  
  INDEX `fk_id_func_veiculo` (`id_func_veiculo` ASC) ,  
  CONSTRAINT `fk_id_func_veiculo`
```

```
FOREIGN KEY (`id_func_veiculo` )  
REFERENCES `controle_rfid`.funcionario (`cod_funcionario` )  
ON DELETE NO ACTION  
ON UPDATE NO ACTION)  
ENGINE = InnoDB;
```

```
CREATE USER 'rfid'@'%' IDENTIFIED BY '12345';  
GRANT ALL PRIVILEGES ON `controle_rfid`. * TO `rfid`@`%`  
WITH GRANT OPTION;
```

